

Leitsätze

zum Beschluss des Ersten Senats vom 10. November 2020

- 1 BvR 3214/15 -

(Antiterrordateigesetz II)

- 1. Regelungen, die den Datenaustausch zwischen Polizeibehörden und Nachrichtendiensten ermöglichen, müssen den besonderen verfassungsrechtlichen Anforderungen der hypothetischen Datenneuerhebung genügen („informationelles Trennungsprinzip“).**
- 2. Das Eingriffsgewicht der gemeinsamen Nutzung einer Verbunddatei der Polizeibehörden und Nachrichtendienste ist bei der „erweiterten Nutzung“ (Data-mining) weiter erhöht.**
- 3. Die erweiterte Nutzung einer Verbunddatei der Polizeibehörden und Nachrichtendienste muss dem Schutz von besonders gewichtigen Rechtsgütern dienen und auf der Grundlage präzise bestimmter und normenklarer Regelungen an hinreichende Eingriffsschwellen gebunden sein.**
 - a. Für die erweiterte Nutzung zur Informationsauswertung muss diese zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten sein; damit wird ein wenigstens der Art nach konkretisiertes und absehbares Geschehen vorausgesetzt.**
 - b. Für die erweiterte Nutzung zur Gefahrenabwehr muss eine wenigstens hinreichend konkretisierte Gefahr gegeben sein.**
 - c. Für die erweiterte Nutzung zur Verfolgung einer Straftat muss ein durch bestimmte Tatsachen begründeter Verdacht vorliegen, für den konkrete und verdichtete Umstände als Tatsachenbasis vorhanden sind.**

BUNDESVERFASSUNGSGERICHT

- 1 BvR 3214/15 -



IM NAMEN DES VOLKES

In dem Verfahren über die Verfassungsbeschwerde

des Herrn S...,

gegen § 6a des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG) vom 22. Dezember 2006 (Bundesgesetzblatt I Seite 3409) in der Fassung des Gesetzes zur Änderung des Antiterrordateigesetzes und anderer Gesetze vom 18. Dezember 2014 (Bundesgesetzblatt I Seite 2318)

hat das Bundesverfassungsgericht – Erster Senat –
unter Mitwirkung der Richterinnen und Richter

Präsident Harbarth,
Paulus,
Baer,
Britz,
Ott,
Christ,
Radtke

am 10. November 2020 beschlossen:

1. **§ 6a Absatz 2 Satz 1 des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG) vom 22. Dezember 2006 (Bundesgesetzblatt I Seite 3409) in der Fassung des Gesetzes zur Änderung des Antiterrordateigesetzes und anderer Gesetze vom 18. Dezember 2014 (Bundesgesetzblatt I Seite 2318) ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar und damit nichtig.**
2. **Im Übrigen wird die Verfassungsbeschwerde zurückgewiesen.**
3. **Die Bundesrepublik Deutschland hat dem Beschwerdeführer seine notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren zur Hälfte zu erstatten.**

G r ü n d e:

A.

Die Verfassungsbeschwerde richtet sich gegen § 6a des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG). 1

I.

1. Durch das 2006 beschlossene Antiterrordateigesetz wurde die Rechtsgrundlage für die Antiterrordatei geschaffen, eine der Bekämpfung des internationalen Terrorismus dienende Verbunddatei von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (vgl. BVerfGE 133, 277 <280 Rn. 3>). Zielsetzung des zugrundeliegenden Gesetzentwurfs war es, „angesichts der Bedrohungen durch den internationalen Terrorismus den Informationsaustausch zwischen Polizeien und Nachrichtendiensten weiter zu verbessern“ (BTDrucks 16/2950, S. 1). 2

Im Regelfall erlaubt § 5 Abs. 1 Nr. 1 Buchstabe a ATDG den gemäß § 1 ATDG berechtigten Behörden bei einer Abfrage zu Personen einen unmittelbaren Zugriff lediglich auf die in der Antiterrordatei zu ihrer Identifizierung gespeicherten Grunddaten wie Name, Geschlecht und Geburtsdatum (§ 3 Abs. 1 Nr. 1 Buchstabe a ATDG). Der Zugriff erstreckt sich nicht auch auf die in der Datei gespeicherten erweiterten Grunddaten (§ 3 Abs. 1 Nr. 1 Buchstabe b ATDG) wie Bankverbindungen, Familienstand und Volkszugehörigkeit; ihn kann erst die Behörde, welche die Daten eingegeben hat, im Einzelfall auf Ersuchen nach den jeweils geltenden Übermittlungsvorschriften gewähren (§ 5 Abs. 1 Satz 3 ATDG). Nur im Eilfall ermöglicht § 5 Abs. 2 Satz 1 ATDG der abfragenden Behörde, unter engen Voraussetzungen unmittelbar auf die erweiterten Grunddaten zu einer Person zuzugreifen und diese zu verwenden, wenn dies zur Abwehr einer gegenwärtigen Gefahr im Zusammenhang mit der Bekämpfung des internationalen Terrorismus unerlässlich ist (§ 6 Abs. 2 ATDG). 3

§ 6a ATDG ist zum 1. Januar 2015 durch das Gesetz zur Änderung des Antiterror-dateigesetzes und anderer Gesetze (im Folgenden: Änderungsgesetz) vom 18. Dezember 2014 (BGBl I S. 2318) in Kraft getreten. Damit einher gingen eine Reihe von Änderungen im Antiterrordateigesetz, nachdem auf eine Verfassungsbeschwerde des Beschwerdeführers der Erste Senat des Bundesverfassungsgerichts mit Urteil vom 24. April 2013 - 1 BvR 1215/07 - (BVerfGE 133, 277 ff.) mehrere Vorschriften der ursprünglichen Gesetzesfassung (im Folgenden: ATDG a.F.) für unvereinbar mit dem Grundgesetz erklärt hatte. Die Antiterrordatei verstieß danach in ihrer ursprünglichen Form insbesondere gegen das informationelle Trennungsprinzip zwischen Nachrichtendiensten und Polizeibehörden.

4

Das Änderungsgesetz diente maßgeblich der Umsetzung des Urteils des Bundesverfassungsgerichts. Im Zuge dessen wurde das Antiterrordateigesetz zugleich erstmalig um die Vorschrift des § 6a ATDG ergänzt, die fast identisch bereits in § 7 des (strukturgleichen) 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) vom 20. August 2012 (BGBl I S. 1798) enthalten ist. Zuvor hatte die Bundesregierung im März 2013 – entsprechend Art. 5 Abs. 2 des Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz a.F.) vom 22. Dezember 2006 (BGBl I S. 3409) – den Bericht zur Evaluierung des Antiterrordateigesetzes vorgelegt (vgl. BTDrucks 17/12665 [neu]). Darin heißt es, dass die Nutzung der Antiterrordatei und die Rückmeldung der Anwender eine Verbesserung der Zusammenarbeit zwischen den Behörden belege und insofern das mit dem Gesetz verfolgte Ziel erreiche, als Instrument zur Bekämpfung des internationalen Terrorismus zu dienen. Sie werde zum Auffinden von Informationen mit Bezug auf den internationalen Terrorismus genutzt und trage dadurch zu Kontakten und Datenflüssen zwischen den Sicherheitsbehörden bei (BTDrucks 17/12665 [neu], S. 5).

5

Indes wurde die fehlende Möglichkeit, Daten innerhalb der Antiterrordatei miteinander zu verknüpfen und weiterführende Analysen zu betreiben, als insgesamt für die Akzeptanz und den Nutzwert der Datei nachteilig wahrgenommen (BTDrucks 17/12665 [neu], S. 54). Aus Sicht ihrer Nutzer, insbesondere der Nachrichtendienste, bedürfe es daher einer Weiterentwicklung. Die Antiterrordatei sollte mit Auswert- und Analysefunktionen versehen werden. Dadurch könnten bereits innerhalb der Verbunddatei weiterführende Erkenntnisse gewonnen und der Informationsaustausch noch besser strukturiert werden (BTDrucks 17/12665 [neu], S. 5). Aus fachlicher Sicht sei es „wünschenswert“, dass zwischen Personen, Gruppierungen und Objekten in der Antiterrordatei Zusammenhänge für Recherchen und Analysen für die weitere Ermittlungsarbeit hergestellt werden könnten (BTDrucks 17/12665 [neu], S. 54). Dies nahm der Gesetzgeber zum Anlass, mit dem Inkrafttreten des Änderungsgesetzes zugleich eine „erweiterte projektbezogene Datennutzung“ in § 6a ATDG zu ermöglichen. Anders als § 7 RED-G a.F. wurde § 6a ATDG nicht mehr mit

6

konkreten Problemen in der Zusammenarbeit von Polizei und Nachrichtendiensten begründet (vgl. dazu BTDrucks 17/8672, S. 19).

In der Praxis wurde die „erweiterte projektbezogene Datennutzung“ bisher soweit ersichtlich weder nach § 6a ATDG noch nach § 7 RED-G angewandt, da die notwendigen technischen Rahmenbedingungen noch nicht hergestellt sind. Nach Auskunft des Bundeskriminalamts gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ist die technische Umsetzung der Anforderungen des § 6a ATDG erst mit einer Umstellung der Antiterrordatei auf einen neuen Softwarekern realisierbar. Einen Termin dafür gebe es noch nicht.

7

2. § 6a ATDG erlaubt unter bestimmten Voraussetzungen im Rahmen eines „Projekts“ eine „erweiterte projektbezogene Nutzung“ der in der Antiterrordatei gespeicherten Grunddaten (§ 3 Abs. 1 Nr. 1 Buchstabe a ATDG), also das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, den Ausschluss unbedeutender Informationen und Erkenntnisse, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten (§ 6a Abs. 5 Satz 1 ATDG). § 6a ATDG gestattet damit die unmittelbare Nutzung der Antiterrordatei nicht bloß zur Vorbereitung eines Auskunftersuchens (§ 6 Abs. 1 Satz 1 Alt. 1 ATDG), sondern zur Generierung neuer Erkenntnisse aus den Querverbindungen der gespeicherten Datensätze.

8

§ 6a ATDG gilt unmittelbar nur für an der Antiterrordatei beteiligte Behörden des Bundes. Sein Absatz 11 enthält allerdings eine Öffnungsklausel für Eingriffsbefugnisse der nach § 1 Abs. 1 ATDG berechtigten Landesbehörden.

9

Die Zulässigkeit der erweiterten Datennutzung in § 6a ATDG wird jeweils an formelle und materielle Kriterien geknüpft.

10

In formeller Hinsicht ist eine schriftliche Anordnung der die Fachaufsicht führenden obersten Behörde erforderlich (§ 6a Abs. 7 ATDG). Zugleich darf eine angeordnete erweiterte Nutzung im Grundsatz nur mit Zustimmung der G 10-Kommission vollzogen werden (§ 6a Abs. 8 ATDG). Nach § 6a Abs. 6 Satz 1 ATDG ist die Zugriffsberechtigung im Rahmen der projektbezogenen erweiterten Nutzung auf die Personen zu beschränken, die unmittelbar mit Arbeiten auf diesem Anwendungsgebiet betraut sind. In zeitlicher Hinsicht begrenzt § 6a Abs. 6 Satz 2 ATDG die Projektdauer auf (höchstens) zwei Jahre, wobei zweimal die Möglichkeit der Verlängerung um jeweils ein Jahr besteht.

11

Materielle Anforderungen ergeben sich aus den in den Absätzen 1 bis 3 enthaltenen Eingriffsregelungen. Diese waren im Gesetzesentwurf zunächst Gegenstand eines einzigen Absatzes (vgl. BTDrucks 18/1565, S. 7). Die Aufteilung in mehrere Absätze erfolgte nach der Sachverständigenanhörung im Innenausschuss. Die Absätze 1 bis 3 unterscheiden danach, ob die erweiterte Nutzung im Rahmen eines bestimmten einzelfallbezogenen Projekts zur Sammlung und Auswertung von Informationen

12

über eine internationale terroristische Bestrebung erforderlich ist, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass Straftaten des internationalen Terrorismus nach den §§ 129a, 129b und 211 des Strafgesetzbuchs (StGB) begangen werden sollen und dadurch Gefahren für Leib, Leben oder Freiheit von Personen drohen (Abs. 1), oder ob die erweiterte Nutzung für die Verfolgung qualifizierter Straftaten des internationalen Terrorismus (Abs. 2 Satz 1) oder ob sie für die Verhinderung von qualifizierten Straftaten (Abs. 3 Satz 1) im Einzelfall erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären. Qualifizierte Straftaten sind Taten des internationalen Terrorismus, die einen Straftatbestand nach den §§ 89a, 89b, 91, 102, 129a, 129b, 211 oder 212 StGB erfüllen (§ 6a Abs. 2 Satz 2, Abs. 3 Satz 2 ATDG). In den Absätzen 4 und 5 definiert der Gesetzgeber die Begriffe Projekt und erweiterte Nutzung.

Die Definition des Projekts wurde nach der Sachverständigenanhörung im Innenausschuss des Deutschen Bundestages in § 6a Abs. 4 ATDG aufgenommen (vgl. zum Gesetzesentwurf BTDrucks 18/1565, S. 7). Hiernach ist ein Projekt eine gegenständlich abgrenzbare und auf bestimmte Zeiträume bezogene Aufgabe, der durch die Gefahr oder den drohenden Schaden, die am Sachverhalt beteiligten Personen, die Zielsetzung der Aufgabe oder deren Folgewirkungen eine besondere Bedeutung zukommt. Zu § 6a Abs. 1, Abs. 2 Satz 1, Abs. 3 Satz 1 ATDG heißt es in der Entwurfsbegründung zum Änderungsgesetz (BTDrucks 18/1565, S. 19):

13

„Ein Einzelfallprojekt zur Sammlung und Auswertung ist nur dann möglich, wenn zu der internationalen terroristischen Bestrebung Tatsachen bekannt sind, welche die Annahme rechtfertigen, dass bestimmte Straftaten des internationalen Terrorismus begangen werden sollen und dass dadurch bestimmte Gefahren drohen. Die Kataloge der in § 6a Absatz 1 aufgeführten Straftaten und Gefahren sind abschließender Natur. Durch diese Einschränkungen ist sichergestellt, dass eine erweiterte Datennutzung nur dann möglich ist, wenn es um „greifbare“ Gefahren für Leib, Leben oder Freiheit von Personen geht. Einzelfallbezogen bedeutet, dass nicht allgemein bestimmte Phänomene oder historische Entwicklungen ausgewertet werden dürfen, sondern das Projekt sich auf konkrete Straftaten, Täter oder Gruppierungen beziehen muss.“

Von der erweiterten Nutzung ausgenommen sind die nach § 4 ATDG verdeckt gespeicherten Daten (§ 6a Abs. 1, Abs. 2 Satz 1, Abs. 3 Satz 1, Abs. 7 Satz 6 ATDG).

14

3. Die angegriffene Vorschrift des § 6a ATDG lautet in ihrer maßgeblichen Fassung vom 18. Dezember 2014, die zum 1. Januar 2015 in Kraft getreten und seither unverändert geblieben ist:

15

§ 6a ATDG

Erweiterte projektbezogene Datennutzung

(1) Eine beteiligte Behörde des Bundes darf zur Erfüllung ihrer gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten erweitert nutzen, soweit dies im Rahmen eines bestimmten einzelfallbezogenen Projekts zur Sammlung und Auswertung von Informationen über eine internationale terroristische Bestrebung, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass Straftaten des internationalen Terrorismus nach den §§ 129a, 129b und 211 des Strafgesetzbuchs begangen werden sollen und dadurch Gefahren für Leib, Leben oder Freiheit von Personen drohen, im Einzelfall erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären.

(2) ¹Eine beteiligte Behörde des Bundes darf zur Erfüllung ihrer gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten erweitert nutzen, soweit dies im Rahmen eines bestimmten einzelfallbezogenen Projekts für die Verfolgung qualifizierter Straftaten des internationalen Terrorismus im Einzelfall erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären. ²Qualifizierte Straftaten des internationalen Terrorismus sind Taten des internationalen Terrorismus, die einen Straftatbestand nach den §§ 89a, 89b, 91, 102, 129a, 129b, 211 oder 212 des Strafgesetzbuchs erfüllen.

(3) ¹Eine beteiligte Behörde des Bundes darf zur Erfüllung ihrer gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten erweitert nutzen, soweit dies im Rahmen eines bestimmten einzelfallbezogenen Projekts für die Verhinderung von qualifizierten Straftaten des internationalen Terrorismus erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären, und Tatsachen die Annahme rechtfertigen, dass eine solche Straftat begangen werden soll. ²Absatz 2 Satz 2 gilt entsprechend.

(4) Ein Projekt ist eine gegenständlich abgrenzbare und auf bestimmte Zeiträume bezogene Aufgabe, der durch die Gefahr oder den drohenden Schaden, die am Sachverhalt beteiligten Personen, die Zielsetzung der Aufgabe oder deren Folgewirkungen eine besondere Bedeutung zukommt.

(5) ¹Eine erweiterte Nutzung sind das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informatio-

nen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten. ²Hierzu dürfen die beteiligten Behörden des Bundes Daten auch mittels

1. phonetischer oder unvollständiger Daten,
2. der Suche über eine Mehrzahl von Datenfeldern,
3. der Verknüpfung von Personen, Institutionen, Organisationen, Sachen oder
4. der zeitlichen Eingrenzung der Suchkriterien

aus der Datei abfragen sowie räumliche und sonstige Beziehungen zwischen Personen und Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen darstellen sowie die Suchkriterien gewichten.

(6) ¹Die Zugriffsberechtigung ist im Rahmen der projektbezogenen erweiterten Nutzung auf die Personen zu beschränken, die unmittelbar mit Arbeiten auf diesem Anwendungsgebiet betraut sind. ²Die projektbezogene erweiterte Nutzung der Datei ist auf höchstens zwei Jahre zu befristen. ³Die Frist kann zweimalig um jeweils bis zu einem Jahr verlängert werden, wenn die Voraussetzungen für die projektbezogene erweiterte Datennutzung fortbestehen und sich aus den mit dem Projekt gewonnenen Erkenntnissen das Bedürfnis für eine Fortführung des Projekts ergibt.

(7) ¹Projektbezogene Datennutzungen dürfen nur auf Antrag angeordnet werden. ²Der Antrag ist durch den Behördenleiter oder seinen Stellvertreter schriftlich zu stellen und zu begründen. ³Er muss alle für die Anordnung erforderlichen Angaben enthalten. ⁴Zuständig für die Anordnung ist die die Fachaufsicht über die antragstellende Behörde führende oberste Bundesbehörde. ⁵Die Anordnung ergeht schriftlich. ⁶In ihr sind der Grund der Anordnung, die für die projektbezogene erweiterte Datennutzung erforderlichen Datenarten nach § 3, der Funktionsumfang und die Dauer der projektbezogenen erweiterten Datennutzung anzugeben. ⁷Der Funktionsumfang der projektbezogenen erweiterten Datennutzung ist auf das zur Erreichung des Projektziels erforderliche Maß zu beschränken. ⁸Die Anordnung ist zu begründen. ⁹Aus der Begründung müssen sich die in den Absätzen 1 bis 3 genannten Voraussetzungen ergeben, insbesondere, dass die projektbezogene erweiterte Nutzung erforderlich ist, um weitere Zusammenhänge aufzuklären. ¹⁰Die anordnende Behörde hält Antrag und Anordnung für datenschutzrechtliche Kontrollzwecke zwei Jahre, mindestens jedoch für die Dauer der projektbezogenen erweiterten Nutzung vor.

(8) ¹Eine nach Absatz 7 angeordnete erweiterte Nutzung darf nur mit Zustimmung der G 10-Kommission (§ 15 Absatz 1 bis 4 des Artikel 10-Gesetzes) vollzogen werden. ²Bei Gefahr im Verzug kann die nach Absatz 7 Satz 4 zuständige Behörde den Vollzug auch bereits vor der Zustimmung der Kommission anordnen. ³Anordnungen, die die Kommission für unzulässig oder nicht notwendig erklärt, hat die nach Absatz 7 Satz 4 zuständige Behörde unverzüglich aufzuheben. ⁴Die aus der erweiterten Datennutzung gewonnenen Daten und Erkenntnisse unterliegen in diesem Fall einem absoluten Verwendungsverbot und sind unverzüglich zu löschen.

(9) Für Verlängerungen nach Absatz 6 Satz 3 gelten die Absätze 7 und 8 entsprechend.

(10) ¹Die alleinige datenschutzrechtliche Verantwortung für die Durchführung des Projekts trägt die antragstellende Behörde. ²Die Übermittlung von aus einem Projekt gewonnenen Erkenntnissen richtet sich nach den allgemeinen Übermittlungsvorschriften. ³§ 6 Absatz 4 Satz 1 gilt für aus einem Projekt nach Absatz 1 gewonnene Erkenntnisse entsprechend.

(11) ¹Die nach § 1 Absatz 1 berechtigten Landesbehörden sind nach Maßgabe landesrechtlicher Regelungen, die den Vorgaben der Absätze 1 bis 10 entsprechen, befugt, die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten zu den in den Absätzen 1 bis 3 genannten Zwecken erweitert zu nutzen. ²Satz 1 gilt auch für Landesbehörden, die durch eine Rechtsverordnung nach § 1 Absatz 2 zur Teilnahme an der Datei berechtigt werden.

4. a) Im Rahmen des Gesetzgebungsverfahrens sprach sich der Bundesrat für eine Streichung des § 6a ATDG aus (BTDrucks 18/1565, S. 25 f.). Diese Vorschrift diene nicht der Umsetzung des Urteils des Bundesverfassungsgerichts zur Antiterrordatei, so dass kein Zeitdruck bestehe. Die Notwendigkeit für eine derartige Regelung, insbesondere für die vorgesehenen Anwendungsfälle, gehe weder aus der Begründung des Gesetzentwurfs noch aus dem dort angesprochenen Evaluationsbericht hinreichend substantiiert hervor. Zudem liege die vorgeschriebene Evaluation des Rechts-
extremismus-Datei-Gesetzes noch nicht vor.

16

Verfassungsrechtlich sei zu bedenken, dass mit der erweiterten Datennutzung die Konzeption der Antiterrordatei als Verbunddatei, die im Kern auf die Informationsanbahnung beschränkt sei und eine Nutzung der Daten zur operativen Aufgabenwahrnehmung nur in dringenden Ausnahmefällen vorsehe, zumindest aufgeweicht werde. Denn die Ausnahme sei nun nicht mehr auf die eng begrenzten Eilfälle im Sinne von § 5 Abs. 2 ATDG beschränkt, sondern umfasse auch bestimmte einzelfallbezogene Projekte. Daneben löse sie sich von dem Prinzip der Einzelabfrage. Beide Elemente

17

seien für die positive Bewertung der Antiterrordatei durch das Bundesverfassungsgericht maßgeblich gewesen. Außerdem sei die Ausgabe von Grunddaten bei Inversuchen durch § 6a ATDG kritisch zu beurteilen. Es bedürfe genauer Prüfung, ob die in § 6a ATDG vorgesehenen sehr hohen inhaltlichen und verfahrensrechtlichen Eingriffsschwellen und die Herausnahme der teilweise besonders sensiblen verdeckt gespeicherten Daten aus dem Anwendungsbereich diese Gesichtspunkte aufwögen.

b) Die im Innenausschuss angehörten Sachverständigen äußerten überwiegend Kritik und verfassungsrechtliche Bedenken. § 6a ATDG verstoße gegen den Verhältnismäßigkeitsgrundsatz und gegen das Gebot der Normenklarheit und -bestimmtheit. Die Vorschrift sei daher verfassungswidrig (vgl. dazu Arzt, Ausschuss-Drucks 18(4)144 A; Bäcker, Ausschuss-Drucks 18(4)144 B; Rossi, Ausschuss-Drucks 18(4)144 F; Wolff, Ausschuss-Drucks 18(4)144 E). Ein Sachverständiger vertrat die Auffassung, dass jedenfalls die materiellen und prozeduralen Hürden, die bereits in § 6a ATDG eingezogen seien, den „zentralen Vorgaben des Bundesverfassungsgerichts nach insbesondere Normenbestimmtheit <...> sehr deutlich“ genügten (vgl. Schwarz, Ausschuss-Drucks 18(4)144 C, S. 10; Wortlautprotokoll der 22. Sitzung des Innenausschusses vom 22. September 2014, Protokoll-Nr. 1822, S. 19).

18

Nach Auffassung der Ständigen Vertreterin des Vizepräsidenten des Bundesamts für Verfassungsschutz ist die Einführung der Datennutzung im Sinne des § 6a ATDG mit einem „erheblichen Mehrwert“ verbunden. Man könne sicherheitsbehördenübergreifend Bezüge herstellen und analysieren, aktuell vor allem bezogen auf Syrienreisende, Irakreisende sowie Terrorismusunterstützer. Die Analyse, die in diesem Zusammenhang oft mühselig durch händische Zusammenstellung von Daten durchgeführt werden müsse, werde deutlich erleichtert, wenn die Antiterrordatei auch dafür genutzt werden könnte. Insbesondere wäre es so möglich, Querschnittsanalysen über Schwerpunkte oder über Kontaktszenarien der Akteure zu erstellen, die wesentliche Ermittlungsansätze für die Aufklärung von Netzwerkstrukturen liefern könnten. Die verfassungsrechtlichen Vorgaben aus der Entscheidung des Bundesverfassungsgerichts seien beachtet (vgl. Rieband, Ausschuss-Drucks 18(4)144 D; Wortlautprotokoll der 22. Sitzung des Innenausschusses vom 22. September 2014, Protokoll-Nr. 1822, S. 12, 24).

19

Der ehemalige Präsident des Bundeskriminalamts sprach sich gleichfalls für das Vorhaben des Gesetzgebers zur „erweiterten Datennutzung“ aus. Angesichts der (aktuellen) Bedrohungslage durch die Terrormiliz Islamischer Staat (IS) und die Rückkehr kampferfahrener Dschihadisten aus Syrien oder dem Irak sei eine Informationsvernetzung weiterhin unabdinglich. Als Projekt sei etwa „an die Finanzierung des Terrorismus, an die Radikalisierung von jungen Leuten in Deutschland, an Schleuserwege – Wie komme man nach Somalia, nach Syrien, al-Nusra oder al-Qaida? –, an Waffendelikte oder an Straftaten aus der rechten Szene zu denken.“ Diese Informationen seien zwar in einem einzelnen Sachverhalt vorhanden, müssten aber in Form eines Projekts gesammelt und analysiert werden. Solche Projekte leisteten einen erheblichen Beitrag zur Aufklärung von Gefahrenlagen (vgl. Ziercke, Ausschuss-

20

Drucks 18(4)144 G; Wortlautprotokoll der 22. Sitzung des Innenausschusses vom 22. September 2014, Protokoll-Nr. 1822, S. 24).

5. Eine Evaluierung des Antiterrordateigesetzes ist unter Geltung des § 6a nicht erfolgt. Nach Inkrafttreten des Änderungsgesetzes und damit auch des § 6a ATDG wurde allerdings das Rechtsextremismus-Datei-Gesetz evaluiert (vgl. BTDrucks 18/8060). Dem Abschlussbericht zufolge bestehen verfassungsrechtliche Bedenken im Hinblick auf die Erforderlichkeit der Regelung, die Vereinbarkeit von § 7 RED-G mit den Anforderungen der Zweckbindung und dem Trennungsprinzip, die verfahrensrechtlichen Absicherungen, die Vereinbarkeit mit dem Übermaßverbot und die Bestimmtheit. Von vornherein verfassungsrechtlich ausgeschlossen dürfte eine solche Regelung jedoch nicht sein (vgl. BTDrucks 18/8060, S. 115 ff.).

21

II.

Der Beschwerdeführer rügt mit seiner Verfassungsbeschwerde, die sich ausschließlich gegen § 6a ATDG richtet, eine Verletzung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

22

1. Die Verfassungsbeschwerde sei zulässig. Insbesondere sei der Beschwerdeführer durch die angegriffene Vorschrift unmittelbar, persönlich und gegenwärtig betroffen. Er beruft sich dabei im Wesentlichen auf die Erwägungen des Bundesverfassungsgerichts im ATDG-Urteil aus dem Jahre 2013 (vgl. BVerfGE 133, 277 <311 ff. Rn. 82 ff.>).

23

Die Verfassungsbeschwerde könne unmittelbar gegen § 6a ATDG gerichtet werden. Zwar bedürfe es noch eines Vollzugsaktes, nämlich der Einstellung seiner Daten in die Antiterrordatei. Doch werde ihm dies nicht zwingend mitgeteilt. Er habe deshalb keine Gelegenheit, vor, während oder nach dem gerügten Grundrechtseingriff eine gerichtliche Kontrolle herbeizuführen. Zwar könne er nach § 10 Abs. 3 ATDG um Auskunft ersuchen und gegebenenfalls dann den Rechtsweg beschreiten. Diese Rechtsschutzmöglichkeit greife aber zu kurz. Selbst wenn ihm an einem Tag mitgeteilt werde, nicht in die Antiterrordatei aufgenommen zu sein, könne schon am nächsten Tag das Gegenteil zutreffen. Zudem seien diese Ersuchen in Bezug auf die verdeckt gespeicherten Daten bei mehr als 40 verschiedenen Behörden zu stellen.

24

Darüber hinaus werde er „mit einiger Wahrscheinlichkeit durch Maßnahmen, die auf der angegriffenen Rechtsnorm beziehungsweise auf §§ 2, 3, 6a ATDG beruhen“, in seinen Grundrechten berührt. Sowohl private oder öffentliche Äußerungen, anonyme Hinweise, ein aus Sicht des Verfassungsschutzes auffälliges Interesse an bestimmten Informationen als auch Beziehungen zu Personen, zu denen er engeren sozialen Umgang pflege, könnten dazu führen, dass ihn Verfassungsschutzbehörden zum Beispiel heimlich belauschten, dabei erlangte Daten speicherten und diese in die Antiterrordatei einstellten. Diese Daten würden damit prinzipiell auch Polizeibehörden zugänglich gemacht, die diese ihn betreffenden Informationen selbst nicht hätten erheben dürfen und ohne das Antiterrordateigesetz nicht zur Kenntnis bekommen hät-

25

ten. Solche Daten würden auch bei der erweiterten projektbezogenen Datennutzung nach § 6a ATDG verwendet.

Gleiches gelte für seine kritischen Äußerungen zu unzulässigen Informationsbeschaffungen der Nachrichtendienste, seine aktive Bekämpfung der Vorratsdatenspeicherung oder seine aktive Unterstützung der „DigitalCourage“; bei allen diesen Bestrebungen könne er – etwa auf Demonstrationen – in Kontakt zu Extremisten und dadurch in das Visier und die Datenspeicherung der Nachrichtendienste geraten sein. Ferner sei es aufgrund seiner in jüngerer Zeit geknüpften Kontakte zu Syrern, die in Berührung mit Kampfhandlungen der Terrororganisation „Islamischer Staat“ gekommen seien, möglich, dass Daten über ihn in der Antiterrordatei gespeichert würden. Dadurch veranlasste oder jedenfalls nicht auszuschließende Speicherungen seiner Daten verletzen sein grundrechtsgleiches Recht auf informationelle Selbstbestimmung.

26

2. Die Verfassungsbeschwerde sei auch begründet. § 6a ATDG, insbesondere dessen Absätze 1 bis 3, verletze sein informationelles Selbstbestimmungsrecht.

27

a) Der Beschwerdeführer könne als unbescholtener Bürger und durch ein völlig legales Verhalten jederzeit in den Blickpunkt der Verfassungsschutzbehörden geraten und zum Objekt nachrichtendienstlicher Informationsbeschaffungen werden. Die gesetzlichen Anforderungen seien besonders gering. Die Schwelle liege weit unterhalb der allgemeinen und polizeilichen Gefahrenabwehr und der Strafverfolgung.

28

Diesem die Grundrechte der Bürger in einem besonderen Maße gefährdenden Zustand trage das sogenannte „Trennungsprinzip“ Rechnung, das Grundrechtseingriffe des Verfassungsschutzes entschärfe. Damit würde verfassungsrechtlich legitimiert, dass die so gewonnenen Daten im Bereich des Verfassungsschutzes zu verbleiben hätten und insbesondere auch nicht den Polizeibehörden zur Verfügung gestellt werden dürften. Andernfalls verschwömmen die Eingriffsbefugnisse der einzelnen Behörden und die Polizei erhalte Informationen, die sie nicht besitzen dürfte, wenn nur die für sie geltenden gesetzlichen Bestimmungen angewendet würden. Letztere würden damit im Ergebnis teilweise ausgehöhlt.

29

Das Trennungsgebot sei vom Bundesverfassungsgericht in der Entscheidung zum Antiterrordateigesetz als Grundsatz anerkannt worden. Das Gericht habe dessen Regelungen mit bestimmten Maßgaben als „ausnahmsweise zulässig“ angesehen. Hierfür habe es entscheidend darauf abgestellt, dass die Antiterrordatei in ihrem Kern auf die Informationsanbahnung beschränkt sei. Nach dem Urteil seien jedoch insbesondere Rasterungen, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern der Antiterrordatei unzulässig.

30

Weil darüber hinaus die über ihn in der Antiterrordatei gespeicherten beziehungsweise jederzeit speicherbaren Daten betroffen seien, verletzen ihn insbesondere § 6a Abs. 1 bis 3 ATDG in seinem Grundrecht auf informationelle Selbstbestimmung.

31

Denn der neue § 6a ATDG diene gerade nicht der Vorbereitung eines Informationsaustauschs. Vielmehr erlaube er einen solchen ausdrücklich, insbesondere in Form einer „übergreifenden Ermittlung von Zusammenhängen zwischen Personen und Verknüpfung von Datenfeldern“ (vgl. § 6a Abs. 5 Satz 2 ATDG). Die Bestimmung gestatte die Gewinnung neuer Informationen durch informationstechnisch nach bestimmten Rastern durchgeführte, umfassende Auswertungen sämtlicher gespeicherter Datenbestände, die polizeiliche und geheimdienstliche Behörden zusammengetragen hätten („Data-mining“). Dies widerspreche der bisherigen und nur so vom Bundesverfassungsgericht im Grundsatz gebilligten Konzeption der Antiterrordatei als einer Verbunddatei, die im Kern auf die Informationsanbahnung beschränkt sei und eine Nutzung der Daten zur operativen Aufgabenwahrnehmung nur in dringenden Ausnahmefällen vorsehe wie im Eilfall nach § 5 Abs. 2 ATDG. § 6a ATDG mache den Datenzugriff dagegen nicht von dessen Unerlässlichkeit abhängig.

Die Eingriffstiefe von § 6a ATDG werde auch nicht dadurch erheblich verringert, dass die Projekte nach Absatz 6 befristet seien. Denn die Frist betrage zwei Jahre und könne zweimal um je ein Jahr verlängert werden, wofür neben dem Fortbestehen der anfänglichen Voraussetzungen lediglich erforderlich sei, dass sich ein „Bedürfnis“ der Fortführung ergebe. Die erweiterte Datennutzung könne folglich auf einen langen Zeitraum von bis zu vier Jahren erstreckt werden. Eine Parallele zu der vom Bundesverfassungsgericht gebilligten „unerlässlichen“ Eilfallregelung (BVerfGE 133, 277 <364 f. Rn. 201 ff.>) bestehe damit gerade nicht.

32

Die Ermöglichung einer langjährigen erweiterten Datennutzung nach § 6a ATDG begründe zudem die „Gefahr, dass sich die zur Eilfallregelung betonte nur ausnahmsweise Überwindung des informationellen Trennungsprinzips zwischen Nachrichtendiensten und Polizei mit besonders schwerem Eingriffsgewicht zu institutionalisieren drohe“. Die neue Qualität, die das Antiterrordateigesetz durch § 6a erfahre, stehe mit den verfassungsrechtlichen Vorgaben nicht in Einklang. § 6a ATDG verstoße gegen das Trennungsgebot und verletze damit das informationelle Selbstbestimmungsrecht des Beschwerdeführers.

33

Die Eingriffstiefe von § 6a ATDG werde auch nicht durch die weiteren formalen Voraussetzungen der erweiterten Datennutzung verringert, etwa durch die Schriftlichkeit des Antrags, die Anordnungsbefugnis der obersten Bundesbehörden oder die personale Eingrenzung der Zugriffsberechtigung. Auch die Erforderlichkeit einer Genehmigung durch die geheim tagende G 10-Kommission sei insoweit ohne Relevanz.

34

b) Darüber hinaus verstoße § 6a ATDG gegen das Gebot der Normenklarheit und -bestimmtheit. Die in § 6a Abs. 4 ATDG enthaltene Definition eines Projekts sei in ihrer vagen sprachlichen Fassung weder verständlich noch bestimmt. Namentlich könne unter einer „Aufgabe“, der „besondere Bedeutung“ zukomme, jede erdenkliche Aufgabe verstanden werden.

35

III.

Zu der Verfassungsbeschwerde haben die Bundesregierung, die damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bayerische Staatsregierung sowie der Bayerische Landesbeauftragte für den Datenschutz Stellung genommen. 36

1. a) Nach Ansicht der Bundesregierung bestehen bereits erhebliche Zweifel an der Zulässigkeit der Verfassungsbeschwerde. Der Beschwerdeführer könne nicht plausibel darlegen, dass er „mit einiger Wahrscheinlichkeit“ durch auf § 6a ATDG beruhende Maßnahmen selbst und gegenwärtig betroffen sein könne. Schon 2013 habe das Bundesverfassungsgericht darauf hingewiesen, dass der Beschwerdeführer „eine spezifische Wahrscheinlichkeit“, von der Speicherung betroffen zu werden, „nur begrenzt“ aufzeigen könne. Das Gericht habe seine Ausführungen seinerzeit nur als „angesichts der großen Streubreite der von der Speicherung in der Antiterrordatei möglicherweise erfassten Personen noch ausreichend“ bezeichnet (BVerfGE 133, 277 <313 Rn. 87>). Der Gesetzgeber habe nach dem Urteil zum Antiterrordateigesetz (a.F.) die darin aufgestellten Anforderungen an den erfassten Personenkreis mit der Neufassung des § 2 ATDG umgesetzt. Nunmehr sei der Kreis potentieller Personen, die in der Datei gespeichert würden, erheblich verringert. Insbesondere die sogenannten „undolosen“ Kontaktpersonen (vgl. § 2 Nr. 3 ATDG a.F.) seien jetzt nicht mehr oder nur verdeckt speicherbar. 37

Folgerichtig müsse die darzulegende Wahrscheinlichkeit einer spezifischen Betroffenheit höher anzusetzen sein. Hier blieben die Ausführungen des Beschwerdeführers, die sich nicht vom Beschwerdevorbringen des vorherigen Verfahrens unterschieden, noch hinter dem zurück, was das Bundesverfassungsgericht 2013 als gerade noch ausreichend angesehen habe. Eine spezifische Wahrscheinlichkeit, von der erweiterten projektbezogenen Datennutzung (§ 6a ATDG) selbst betroffen zu sein, lege der Beschwerdeführer nunmehr nicht einmal mehr „begrenzt“, sondern überhaupt nicht mehr dar. 38

b) Die Verfassungsbeschwerde sei jedenfalls unbegründet, weil § 6a ATDG mit dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) vereinbar und insbesondere auch verhältnismäßig und hinreichend bestimmt sei. § 6a ATDG sei in den Tatbestandsvoraussetzungen sehr eng gefasst. Dass der Zugriff der Daten nicht „unerlässlich“ im Sinne der Eilfallregelung (§ 5 Abs. 2 ATDG) sein müsse, sei unerheblich, denn dies werde durch die Absätze 6 bis 8 kompensiert. 39

Entgegen der Auffassung des Beschwerdeführers sei die in § 6a Abs. 4 ATDG enthaltene Legaldefinition des „Projekts“ auch nicht zu unbestimmt. Projekte zur Bekämpfung des internationalen Terrorismus seien ihrer Natur nach ganz unterschiedlich und erforderten mit Blick auf die Eigenart der Materie Raum für die Berücksichtigung zahlreicher im Voraus nicht normierter Gesichtspunkte durch die Behörden. Eine noch bestimmtere Wortfassung als die von § 6a Abs. 4 ATDG sei 40

deshalb schwer vorstellbar. Der Gesetzgeber habe den Begriff des „Projekts“ aus der Organisationslehre übernommen. „Projekt“ sei dort ein inhaltlich klarer Begriff, der in Abgrenzung zu allgemeinen Daueraufgaben eine im Ziel spezielle, zeitlich begrenzte und in der Durchführung besonders organisierte, hierdurch begrenzte Aufgabe zum Gegenstand habe. Hier gehe es um ein besonderes Erkenntnisziel jenseits der allgemeinen Daueraufgaben. Die Zusätze „bestimmte einzelfallbezogene“ in den Absätzen 1 bis 3 des § 6a ATDG bekräftigten den Projektcharakter. In den Absätzen 1 bis 3 des § 6a ATDG erschließe sich außerdem, dass Projektgegenstand jeweils die Aufklärung bestimmter Straftaten sei, auch hinsichtlich weiterer Zusammenhänge oder einer konkretisierten Gefahr und der Verhinderung ihrer Realisierung. Es gehe also jeweils um konkretisierte Lebenssachverhalte, die projekthaft mit dem Ziel der Störungsverhinderung oder Strafverfolgung aufgeklärt würden.

Auch das Kriterium der „besonderen Bedeutung“ (§ 6a Abs. 4 ATDG) sei hinreichend bestimmt. Es verdeutliche, dass unter Projekt keine Routineaufgaben zu verstehen seien wie etwa die Erstellung eines Lagebildes beim Bundeskriminalamt. Umstände, die zur besonderen Bedeutung eines Projekts führten, würden in § 6a Abs. 1 bis 3 ATDG hinreichend bestimmt beschrieben. Die besondere Bedeutung ergebe sich aus den in § 6a Abs. 1 bis 3 ATDG aufgeführten tatbestandlichen Voraussetzungen. 41

2. Die frühere Bundesbeauftragte für den Datenschutz und die Informationsfreiheit äußerte verfassungsrechtliche Bedenken. Die Formulierung des § 6a ATDG zur erweiterten Datennutzung stelle nicht nur eine besondere Form der Auswertung, sondern ein neues Datenmodell dar. Dieses entspreche den zunehmend neu eingeführten ereignisorientierten Datenbanken. 42

§ 6a ATDG durchbreche das informationelle Trennungsprinzip. Der Grundrechtseingriff sei daher erheblich und nicht gerechtfertigt. Insbesondere reiche es für die Annahme der verfassungsrechtlich gebotenen Erforderlichkeit der Norm nicht aus, dass diese als sinnvoll erachtet werde. Die von der Bundesregierung behauptete Notwendigkeit und Dringlichkeit sei nicht nachvollziehbar. Die bisher nicht erfolgte Anwendung der mit § 6a ATDG geschaffenen Befugnisse untermauere die Kritik. Den verfassungsrechtlichen Vorgaben der Entscheidung des Bundesverfassungsgerichts von 2013 werde nicht Rechnung getragen. Darin habe es zu § 5 ATDG ausgeführt, dass die Zugriffsbefugnis auf die in der Antiterrordatei gespeicherten personenbezogenen Daten unter anderem deshalb verfassungsgemäß sei, da sie lediglich Einzelabfragen erlaube, nicht aber auch eine Rasterung, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern (BVerfGE 133, 277 <361 Rn. 194>). Zudem habe es das Gericht als verfassungsgemäße Begrenzung angesehen, dass keine Abfrage mit unvollständigen Daten möglich sei. 43

Mit den in § 6a ATDG normierten erweiterten projektbezogenen Datennutzungen könnten nun aber die in der Antiterrordatei gespeicherten Daten analysiert und hier- 44

aus neue Erkenntnisse (sogenannte Mehrwerte) gewonnen werden. Diese Nutzungsmöglichkeit erweitere erheblich die grundsätzlich auf Informationsanbahnung beschränkte Funktion der Antiterrordatei. Das Bundesverfassungsgericht habe gerade aus dieser Funktionsbeschränkung eine entscheidende Minderung des Eingriffsgewichts der Antiterrordatei gefolgert, zumal bereits die Aufnahme in eine solche Datei für die Betroffenen erheblich belastende Wirkung haben könne und sich aus dieser Speicherung für die Betroffenen weitreichende Konsequenzen ergeben könnten.

Mit Blick auf § 6a Abs. 4 ATDG sei nicht ersichtlich, wann eine „besondere Bedeutung“ im Sinne der Legaldefinition des „Projektes“ gegeben sei. Terrorismusbekämpfung habe immer eine besondere Bedeutung. Nicht klar sei daher, wie sich die besondere Bedeutung des Projekts von der stets gegebenen Bedeutung abgrenzen solle. Es sei fraglich, ob überhaupt ein der Aufgabenerfüllung dienender Sachverhalt vorstellbar sei, der sich nicht unter § 6a Abs. 4 ATDG subsumieren lasse. Gleichfalls fraglich sei, welche Daten überhaupt miteinander abgeglichen werden dürften, insbesondere ob § 6a ATDG lediglich einen internen Datenabgleich erlauben wolle oder ob nach § 6a Abs. 5 Satz 2 ATDG Datenverarbeitungen außerhalb der Antiterrordatei in den Abgleich einzubeziehen seien. Eine Verknüpfung sei jedoch mit einer weiteren Speicherung verbunden. Im Ergebnis regle § 6a ATDG ein neues Datenmodell, das den zunehmend neu eingeführten ereignisorientierten Datenbanken entspreche.

45

3. Die Bayerische Staatsregierung teilt die Ansicht der Bundesregierung, die Verfassungsbeschwerde sei unzulässig; jedenfalls aber sei sie unbegründet. § 6a ATDG genüge den vom Bundesverfassungsgericht formulierten strengen Anforderungen an einen ausnahmsweise zulässigen Austausch personenbezogener Daten zwischen Polizei und Nachrichtendiensten. Das gelte unabhängig davon, ob der im Urteil von 2013 zugrunde gelegte Maßstab für die Zulässigkeit eines Datenaustauschs zwischen Polizei und Nachrichtendiensten oder die im Urteil des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz (BVerfGE 141, 220 ff.) fortentwickelten Grundsätze für maßgeblich erachtet würden.

46

Die im Urteil zum Antiterrordateigesetz von 2013 vorgenommene Typisierung der Aufgaben und Befugnisse von Polizei und Verfassungsschutz sei zu überdenken. Tatsächlich bestünden erhebliche Überschneidungen der Aufgabenbereiche. Darüber hinaus sei zu erwägen, den Maßstab aus dem Urteil des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz anzuwenden. Danach dürften Daten zwischen den Sicherheitsbehörden grundsätzlich ausgetauscht werden, wenn es sich um Informationen handele, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie diejenigen ergäben, zu deren Schutz die entsprechende Datenerhebung zulässig sei. § 6a ATDG genüge dann erst recht den verfassungsrechtlichen Anforderungen.

47

Trotz des qualitativen Unterschieds zwischen dem „normalen“ Zugriff auf die in der

48

Antiterrordatei gespeicherten Daten nach § 5 ATDG und der erweiterten projektbezogenen Nutzung nach § 6a ATDG bestünden gegen die Datennutzung nach § 6a ATDG keine verfassungsrechtlichen Bedenken. Der Gesetzgeber habe durch sehr restriktive Voraussetzungen sichergestellt, dass die Voraussetzungen für die Datenübermittlung im Einzelfall stets gewahrt blieben. Die gesetzlichen Anforderungen des § 6a ATDG antizipierten damit gleichsam die sonst nach § 5 Abs. 1 ATDG anzustellende Prüfung der Übermittlungsvoraussetzungen.

Das verfassungsrechtliche Gewicht der Zwecke, zu denen eine solche erweiterte projektbezogene Nutzung zulässig sei, entspreche mindestens dem Gewicht der Datenspeicherung in der Antiterrordatei. Bei § 6a Abs. 1 ATDG würden die Daten nur zum Schutze höchster Rechtsgüter genutzt. Auch bei § 6a Abs. 2 und 3 ATDG gehe es um Straftaten, die höchste Schutzgüter betreffen und mithin zu den Verfassungsgütern von besonders hohem Rang zählten. Dabei erforderten sowohl die Einstellung der Daten in die Antiterrordatei als auch ihr Abruf zur erweiterten projektbezogenen Nutzung eine hinreichende Tatsachenbasis. Damit sei sichergestellt, dass die Daten nicht unter dem Stichwort „Terrorismusbekämpfung“ beliebig abgerufen werden könnten. Limitierend komme außerdem hinzu, dass die erweiterte Nutzung auf Projekte beschränkt sei, die gegenständlich und zeitlich begrenzt seien (§ 6a Abs. 4 ATDG). Dadurch werde der Datenabruf wieder stark an die einzelfallbezogene Datenübermittlung angenähert. Flankiert werde die Befugnis zur erweiterten Nutzung außerdem durch strenge Verfahrensvorschriften, insbesondere das Erfordernis der Zustimmung durch die G 10-Kommission (§ 6a Abs. 8 ATDG).

49

4. Demgegenüber hebt der Bayerische Landesbeauftragte für den Datenschutz hervor, § 6a ATDG ziele strukturell auf die Schaffung von Dateien ab, die den polizeilichen Falldateien ähnelten. Derartige Falldateien sollten insbesondere dazu beitragen, die Strukturen organisierter Kriminalität aufzudecken. Dementsprechend beschränkten sich diese Dateien nicht nur auf personenbezogene Daten, die sich in erster Linie auf ein konkretes Zielprojekt (zum Beispiel eine Person) bezögen. Vielmehr würden Daten typischerweise aus allen möglichen Ermittlungsverfahren zu einem Deliktsbereich zusammengetragen, um etwa eventuell übereinstimmende Tatbehebungsmuster aufzudecken. Diese Zielsetzung bilde der letzte Halbsatz in § 6a Abs. 1 ATDG ab.

50

Der Landesbeauftragte gibt zu bedenken, dass jedenfalls in der polizeilichen Praxis zu befürchten sei, dass der Einzelfall im Sinne des § 6a Abs. 1 ATDG regelmäßig sehr weit angewendet werde. Projektbezogene Daten im Sinne von § 6a ATDG dürften sich nur insoweit wesentlich von den polizeilichen Falldateien unterscheiden, als auch Nachrichtendienste zu dem Kreis der Zugriffsberechtigten gehörten.

51

Bislang könne er nicht erkennen, dass die Antiterrordatei einen nennenswerten Nutzen für die Sicherheitsbehörden des Freistaats Bayern erbringe. Es liege die Vermutung nahe, dass diese Einschätzung auch für die Sicherheitsbehörden des Bundes gelte. § 6a ATDG versuche insoweit, das ungünstige Verhältnis zwischen erhebli-

52

chem Befüllungs- und Pflegeaufwand einerseits und geringem Nutzen andererseits zu verändern, indem die Nutzungsmöglichkeiten der Datei erweitert würden.

B.

Die Verfassungsbeschwerde, welche § 6a ATDG in Gänze angreift, ist zulässig. Der Beschwerdeführer ist beschwerdebefugt (I). Das Subsidiaritätserfordernis ist gewahrt (II). Schließlich ist die Materie nicht vom Unionsrecht determiniert und damit einer Entscheidung des Bundesverfassungsgerichts zugänglich (III). 53

I.

Der Beschwerdeführer ist beschwerdebefugt (vgl. Art. 93 Abs. 1 Nr. 4a GG, § 90 Abs. 1 BVerfGG). Eine Verletzung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG erscheint auf Grundlage seiner Angaben möglich (1). Unter Berücksichtigung der Unkenntnis der eingestellten Daten und der Streubreite der Datennutzung ist der Beschwerdeführer auch unmittelbar, selbst und gegenwärtig betroffen (2). 54

1. Der Beschwerdeführer macht eine mögliche Verletzung des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG durch Speicherung und Verwendung seiner Daten geltend. Das Recht auf informationelle Selbstbestimmung schützt auch vor der Verknüpfung von Datenbeständen (vgl. zum Gewährleistungsgehalt BVerfGE 133, 277 <317 Rn. 95>), wie sie § 6a Abs. 1 bis 3 ATDG im Wege der erweiterten projektbezogenen Datennutzung vorsieht. 55

2. Die angegriffene Vorschrift betrifft den Beschwerdeführer unmittelbar, selbst und gegenwärtig. Seine Verfassungsbeschwerde erfüllt auch die spezifischen Anforderungen, die für unmittelbar gegen Gesetze gerichtete Verfassungsbeschwerden gelten. 56

a) Zwar ist ein Beschwerdeführer nur dann von einer gesetzlichen Regelung unmittelbar betroffen, wenn diese in seinen Rechtskreis eingreift, ohne dass es eines weiteren Vollzugsaktes bedürfte. Erfordert das Gesetz zu seiner Durchführung rechtsnotwendig oder auch nur nach der tatsächlichen staatlichen Praxis einen besonderen, vom Willen der vollziehenden Stelle beeinflussten Vollzugsakt, müssen Beschwerdeführende grundsätzlich zunächst diesen Akt angreifen und den gegen ihn eröffneten Rechtsweg erschöpfen, bevor sie Verfassungsbeschwerde erheben (vgl. BVerfGE 1, 97 <101 ff.>; 109, 279 <306>; stRspr). Von einer unmittelbaren Betroffenheit durch ein vollziehungsbedürftiges Gesetz ist aber 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 150, 309 <324 Rn. 35>; stRspr). Der Beschwerdeführer erlangt hier durch ein an das Bundeskriminalamt oder eine beteiligte Behörde zu richtendes Auskunftsverlangen nach § 10 Abs. 3 ATDG weder von den über ihn gespeicherten Daten selbst noch über deren erweiterte Nut-

zung verlässlich Kenntnis (vgl. auch BVerfGE 133, 277 <312 Rn. 84>; 150, 309 <324 f. Rn. 36>).

b) Der Beschwerdeführer ist durch die angegriffene Regelung auch selbst betroffen. Da er weithin keine verlässliche Kenntnis von den Vollzugsakten erlangt, genügt es, wenn er darlegt, mit einiger Wahrscheinlichkeit von solchen Maßnahmen berührt zu werden. Dies hat er hier noch ausreichend getan. 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.>; 133, 277 <312 Rn. 86>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 75 - Bestandsdatenauskunft II).

58

c) Der Beschwerdeführer ist von der angegriffenen Regelung auch gegenwärtig betroffen (vgl. dazu auch BVerfGE 64, 301 <319>), obwohl § 6a ATDG soweit ersichtlich noch nicht zur Anwendung gekommen ist. Die Bundesregierung hat nicht vorgebracht, die Befugnisse aus § 6a ATDG endgültig nicht mehr nutzen zu wollen, sondern nur, dass bisher keine Projekte initiiert oder durchgeführt worden seien. Die technischen Voraussetzungen können jederzeit geschaffen werden, ohne dass die Öffentlichkeit oder der Beschwerdeführer hiervon Kenntnis erlangten, ebenso wenig wie von Datenspeicherungen und der erweiterten projektbezogenen Nutzung dieser Daten nach § 6a Abs. 1 bis 3 ATDG. Daher steht die bislang unterbliebene Anwendung der angegriffenen Norm der Zulässigkeit der Verfassungsbeschwerde nicht entgegen.

59

II.

Die Verfassungsbeschwerde genügt den Anforderungen der Subsidiarität (§ 90 Abs. 2 BVerfGG). Auch vor Erhebung von Rechtssatzverfassungsbeschwerden sind grundsätzlich alle Mittel zu ergreifen, die der geltend gemachten Grundrechtsverletzung abhelfen können. Zu den zumutbaren Rechtsbehelfen kann die Erhebung einer Feststellungs- oder Unterlassungsklage gehören, die eine fachgerichtliche Klärung entscheidungserheblicher Tatsachen- oder Rechtsfragen des einfachen Rechts ermöglicht (vgl. BVerfGE 150, 309 <326 ff. Rn. 41 ff.>; stRspr). Anders liegt dies jedoch, soweit es allein um die sich unmittelbar aus der Verfassung ergebenden Grenzen für die Auslegung der Normen geht. Soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung nicht (vgl. BVerfGE 123, 148 <172 f.>; 143, 246 <322 Rn. 211>; 150, 309 <326 f. Rn. 44>; stRspr). Eine Pflicht zur Anrufung der Fachgerichte kann auch sonst unzumutbar sein (vgl. BVerfGE 150, 309 <327 f. Rn. 45>).

60

Danach musste der Beschwerdeführer vor Erhebung der Verfassungsbeschwerde keinen fachgerichtlichen Rechtsschutz gegen die angegriffene Vorschrift suchen. Die ausschließlich gegen § 6a ATDG 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. Angesichts der Legaldefinition des Projekts in § 6a Abs. 4 ATDG ist auch diesbezüglich keine weitere fachgerichtliche Klärung zu erwarten. 61

Dass der Beschwerdeführer gemäß § 10 Abs. 3 ATDG auf Antrag die Möglichkeit hat, Auskunft über die Speicherung der Daten zu erhalten und anschließend gegen die Speicherung die Gerichte anzurufen, steht dem Grundsatz der Subsidiarität gleichfalls nicht entgegen. Denn auf diesem Weg kann er lediglich dagegen gerichtlich vorgehen, dass zu einem bestimmten Zeitpunkt Daten über ihn tatsächlich gespeichert sind, nicht aber dagegen, dass eine Speicherung jederzeit erneut möglich ist, ohne dass er hierauf Einfluss hätte oder hiervon Kenntnis erlangte. Die Möglichkeit, eine Verfassungsbeschwerde unmittelbar gegen ein Gesetz zu erheben, das zu heimlichen Maßnahmen berechtigt, entfällt jedenfalls in der Regel nur dann, wenn die Betroffenen durch eine aktive Informationspflicht des Staates rechtlich gesichert von der Maßnahme später Kenntnis erlangen (vgl. BVerfGE 133, 277 <312 Rn. 84>). Eine solche Informationspflicht sieht das Antiterrordateigesetz indes weder für die Speicherung der Daten noch für deren Nutzung auf der Grundlage von § 6a ATDG vor. 62

III.

Die Zuständigkeit des Bundesverfassungsgerichts für die Prüfung am Maßstab der Grundrechte des Grundgesetzes ist eröffnet, da § 6a ATDG kein zwingendes Unionsrecht in deutsches Recht umsetzt (vgl. bereits BVerfGE 133, 277 <313 ff. Rn. 88 ff.>). Rechtsvorschriften der Europäischen Union enthalten keine Bestimmungen, welche die Einrichtung einer Antiterrordatei von Polizeibehörden und Nachrichtendiensten erforderten oder gar abschließend regelten. 63

1. Die Verfassungsbeschwerde wäre nur unzulässig, wenn Vorschriften zu überprüfen wären, die durch das Unionsrecht vollständig determiniert sind. Das Bundesverfassungsgericht übt grundsätzlich keine Kontrolle über unionsrechtliches Fachrecht aus und überprüft dieses Recht nicht am Maßstab der Grundrechte des Grundgesetzes, solange die Unionsgrundrechte einen wirksamen Schutz der Grundrechte generell bieten, der dem vom Grundgesetz jeweils als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen gleich zu achten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt; maßgeblich ist insoweit eine auf das jeweilige Grundrecht des Grundgesetzes bezogene generelle Betrachtung (vgl. BVerfGE 73, 339 <387>; 102, 147 <162 f.>; 125, 260 <306>; 152, 216 <235 f. Rn. 47 a.E.>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 84 – Bestandsdatenauskunft II). Diese Grundsätze gelten auch für die Über- 64

prüfung innerstaatlicher Rechtsvorschriften, die zwingende Vorgaben in deutsches Recht umsetzen (vgl. BVerfGE 118, 79 <95 ff.>; BVerfG, Beschluss des Zweiten Senats vom 11. März 2020 - 2 BvL 5/17 -, Rn. 65). Verfassungsbeschwerden, die sich gegen in diesem Sinne verbindliches Fachrecht der Europäischen Union richten, sind danach grundsätzlich unzulässig (vgl. BVerfGE 118, 79 <95>; 152, 216 <237 Rn. 51>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 84 – Bestandsdatenauskunft II).

Handelt es sich aber wie hier um innerstaatliche Normen im nicht oder nicht vollständig vereinheitlichten Bereich, prüft das Bundesverfassungsgericht die angegriffenen Normen am Maßstab der Grundrechte des Grundgesetzes. Das gilt unabhängig davon, ob und wieweit die angegriffenen Vorschriften nach der Rechtsprechung des Gerichtshofs der Europäischen Union zugleich als Durchführung des Unionsrechts im Sinne des Art. 51 Abs. 1 Satz 1 GRCh angesehen werden könnten (vgl. dazu aber BVerfGE 133, 277 <315 Rn. 90>) und deshalb daneben auch die Unionsgrundrechte Geltung beanspruchen könnten (vgl. BVerfGE 152, 152 <168 Rn. 39>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 87, 261 – Bestandsdatenauskunft II).

65

2. Danach ist die angegriffene Vorschrift am Maßstab des Grundgesetzes zu überprüfen, denn sie dient von vornherein nicht der Umsetzung von Unionsrecht. Eine unionsrechtliche Determinierung ergibt sich weder aus der „ePrivacy“-Richtlinie noch aus der JI-Datenschutzrichtlinie noch aus der Terrorbekämpfungs-Richtlinie.

66

Unabhängig von der Frage ihrer generellen Anwendbarkeit auf Sicherheits- und Nachrichtendienste im Lichte von Art. 4 Abs. 2 Satz 3 EUV bezieht sich die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, „ePrivacy“-Richtlinie [ABl. L 201 vom 31. Juli 2002, S. 37]) nach ihrem Art. 1 Abs. 1 nur auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Union und damit nicht auf die staatliche Nutzung von den Sicherheitsbehörden gespeicherter Daten (vgl. EuGH, Urteil vom 6. Oktober 2020, Privacy International, C-623/17, EU:C:2020:790, Rn. 48; Urteil vom 6. Oktober 2020, La Quadrature du Net, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 103).

67

Die 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. L 119 vom 4. Mai 2016, S. 89, im Folgenden: JI-DatenschutzRL) enthält ausweislich ihres Art. 1 Abs. 1 Bestimmungen zum Schutz natürlicher Personen bei

68

der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Art. 8 JI-DatenschutzRL verlangt die Erforderlichkeit einer Datenverarbeitung für die Aufgabenerfüllung der zuständigen Behörde zu den Zwecken der Strafverfolgung und der Gefahrenabwehr gemäß Art. 1 Abs. 1 JI-DatenschutzRL. Art. 11 JI-DatenschutzRL schließt nachteilige Folgen automatischer Datenverarbeitung ohne gesetzliche Grundlage und Garantien für die Rechte und Freiheiten der betroffenen Person aus, Art. 12 ff. JI-DatenschutzRL regeln Rechte der betroffenen Person, Art. 19 ff. JI-DatenschutzRL die Pflichten der Verantwortlichen und Auftragsverarbeiter. § 6a ATDG dient offensichtlich nicht der Umsetzung dieser Maßgaben, die weiterhin keine Vorgaben für die Einrichtung und Ausgestaltung einer Antiterrordatei und die Verarbeitung dieser Daten enthalten (vgl. bereits BVerfGE 133, 277 <315 Rn. 90>).

Die Terrorismusbekämpfungs-Richtlinie [Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. L 88 vom 31. März 2017, S. 6), im Folgenden: TerrorismusbekämpfungsRL] enthält nach ihrem Artikel 1 „Mindestvorschriften für die Definition von Straftatbeständen und die Festlegung von Sanktionen auf dem Gebiet von terroristischen Straftaten, Straftaten im Zusammenhang mit einer terroristischen Vereinigung und Straftaten im Zusammenhang mit terroristischen Aktivitäten sowie Maßnahmen zum Schutz, zur Unterstützung und zur Hilfe der Opfer des Terrorismus.“ Keine der Vorschriften betrifft unmittelbar die Gefahrenabwehr oder auch die Strafverfolgung als solche. Art. 20 TerrorismusbekämpfungsRL stellt lediglich fest, dass die Mitgliedstaaten die erforderlichen Maßnahmen treffen, damit wirksame Ermittlungsinstrumente zur Verfügung stehen. Art. 2 des Beschlusses 2005/671/JI des Rates vom 20. September 2005 über den Informationsaustausch und die Zusammenarbeit betreffend terroristische Straftaten (ABl. L 253 vom 29. September 2005, S. 22 in der Fassung der TerrorismusbekämpfungsRL) sieht vor, dass die Mitgliedstaaten nach Maßgabe der innerstaatlichen Vorschriften alle einschlägigen Informationen über die von ihren Strafverfolgungsbehörden durchgeführten Ermittlungen zu terroristischen Straftaten und über deren Ergebnisse an Eurojust, Europol und die anderen Mitgliedstaaten weiterzuleiten haben. Der Beschluss verpflichtet die Mitgliedstaaten weder zur Einrichtung und Regulierung von Antiterrordateien und deren Verarbeitung noch macht er ihnen sonst hierzu abschließende Vorgaben.

69

C.

Die Verfassungsbeschwerde ist teilweise begründet. Die erweiterte projektbezogene Datennutzung nach § 6a ATDG greift in das Recht des Beschwerdeführers auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ein (I). Die Regelung ist zwar formell verfassungsgemäß (II), aber in ihrer Ausge-

70

staltung in Absatz 2 Satz 1 unverhältnismäßig (III).

I.

Das Recht auf informationelle Selbstbestimmung trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich unter den Bedingungen moderner Datenverarbeitung aus informationsbezogenen Maßnahmen ergeben (vgl. BVerfGE 65, 1 <42 f.>; stRspr). Die freie Entfaltung der Persönlichkeit setzt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist von dem Grundrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Die Gewährleistung greift insbesondere, wenn die Entfaltung der Persönlichkeit dadurch gefährdet wird, dass personenbezogene Informationen von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene weder überschauen noch beherrschen können (vgl. BVerfGE 118, 168 <184>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 92 m.w.N. – Bestandsdatenauskunft II).

71

§ 6a Abs. 1 bis 3 ATDG greift in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ein, indem er den beteiligten Behörden eine erweiterte projektbezogene Nutzung der in der Datei nach § 3 ATDG gespeicherten Datenarten erlaubt (zum Eingriffscharakter der Weiterverwendung von Daten BVerfGE 133, 277 <317 Rn. 95>; stRspr).

72

Der Eingriff liegt hier nicht nur in der weiteren Verwendung vormals getrennter Daten, sondern in dem darüber hinausgehenden Zugriff, den die „erweiterte Nutzung“ ermöglicht. § 6a Abs. 5 Satz 1 ATDG beschreibt diese als „das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, de[n] Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten.“ Die beteiligten Behörden können damit aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen (vgl. § 6a Abs. 5 Satz 2 ATDG) sowie aus der Datenauswertung neue Zusammenhänge erschließen. Die Verknüpfung von Daten ermöglicht etwa mehrstufige Analysen, die neue Verdachtsmomente erst erzeugen, sowie weitere Analyseschritte oder auch daran anschließende operative Maßnahmen. Die Nachteile, die Betroffenen auf Grund einer Maßnahme nach § 6a ATDG drohen, können daher erheblich sein und das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen (vgl. zur insoweit vergleichbaren Rasterfahndung auch BVerfGE 115, 320 <347, 351 ff.>).

73

Bei der in § 6a ATDG geregelten „erweiterten projektbezogenen Datennutzung“ handelt es sich damit um einen typischen Fall von „Data-mining“. Ein solches liegt nach einer Definition der Bundesregierung vor, wenn Verfahren und Methoden ein-

74

gesetzt werden, „mit deren Hilfe bereits vorhandene große Datenbestände, zumeist auf statistisch-mathematischen Verfahren basierend, selbständig auf Zusammenhänge analysiert werden, um auf diesem Wege ‚neues Wissen‘ zu generieren“ (Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jelpke et al. und der Fraktion DIE LINKE, BTDrucks 17/11582, S. 3). Vor Einfügung des § 6a ATDG war eine solche erweiterte Nutzung nicht erlaubt. Eine Rasterung, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern sah das Antiterrordateigesetz bislang gerade nicht vor (vgl. BVerfGE 133, 277 <361 Rn. 194>). Die Nutzung der Antiterrordatei war darüber hinaus auf die Informationsanbahnung beschränkt. Lediglich in Eilfällen erlaubten § 5 Abs. 2, § 6 Abs. 2 ATDG den Zugriff auf (erweiterte) Grunddaten und deren Verwendung auch zur operativen Aufgabenwahrnehmung.

II.

In Grundrechte darf nur durch ein insgesamt verfassungsmäßiges Gesetz eingegriffen werden (vgl. BVerfGE 6, 32 <37 ff.>; 80, 137 <153>; stRspr). Das schließt die formelle Verfassungsmäßigkeit, insbesondere die Gesetzgebungszuständigkeit des Bundes, ein. Der Bund ist für § 6a ATDG gemäß Art. 73 Abs. 1 Nr. 10 GG (1) und Art. 73 Abs. 1 Nr. 1 und 5 GG (2) zuständig.

75

1. a) Soweit das Gesetz die erweiterte projektbezogene Datennutzung durch das Bundeskriminalamt, das Bundesamt für Verfassungsschutz sowie die Öffnung der Daten für die erweiterte Nutzung durch die Landeskriminalämter und die Landesverfassungsschutzbehörden (vgl. § 6a Abs. 11 ATDG) regelt, folgt die Kompetenz zur Regelung der behördlichen Zusammenarbeit aus Art. 73 Abs. 1 Nr. 10 Buchstabe a bis c GG. Diese Zusammenarbeit umfasst die laufende gegenseitige Unterrichtung und Auskunftserteilung, die wechselseitige Beratung sowie gegenseitige Unterstützung und Hilfeleistung in den Grenzen der je eigenen Befugnisse und erlaubt funktionelle und organisatorische Verbindungen, gemeinschaftliche Einrichtungen und gemeinsame Informationssysteme. Hierunter fällt auch die durch das Antiterrordateigesetz vorgesehene Zusammenarbeit (vgl. BVerfGE 133, 277 <317 f. Rn. 96 ff.>).

76

Die Kompetenz für die Zusammenarbeit zwischen den verschiedenen Polizeibehörden beschränkt sich dabei nicht auf die Strafverfolgung. Art. 73 Abs. 1 Nr. 10 GG soll die Möglichkeit schaffen, föderale Zuständigkeitsgrenzen bei der Erfüllung repressiver und präventiver Aufgaben zu lockern. 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>). Art. 73 Abs. 1 Nr. 10 GG erlaubt solche fachübergreifenden Regelungen (vgl. ausführlich BVerfGE 133, 277 <318 Rn. 99> m.w.N.). 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

77

oder die Bekämpfung von Kleinkriminalität, erst recht die Bekämpfung von Ordnungswidrigkeiten.

b) Demnach bestehen an einer Bundeskompetenz aus Art. 73 Abs. 1 Nr. 10 GG mit Blick auf § 6a ATDG keine Bedenken. Insbesondere hat sich der Gesetzgeber in dessen Absätzen 1 bis 3 „auf bedeutsame Straftaten von Gewicht“ im vorgenannten Sinne beschränkt. Straftaten (des internationalen Terrorismus) gemäß § 129a StGB (Bildung terroristischer Vereinigungen), § 129b StGB (Kriminelle und terroristische Vereinigungen im Ausland) und § 211 StGB (Mord) (§ 6a Abs. 1 und 2 Satz 2 ATDG) erfüllen die Voraussetzungen des Art. 73 Abs. 1 Nr. 10 GG ebenso wie § 212 StGB (Totschlag), § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat), § 89b StGB (Aufnahme von Beziehungen zur Begehung einer solchen Tat), § 91 StGB (Anleitung zur Begehung einer solchen Tat) und § 102 StGB (Angriffe gegen Organe und Vertreter ausländischer Staaten), die bei § 6a Abs. 2 und 3 ATDG hinzukommen. Auch letztere Strafvorschrift bezieht sich auf Angriffe auf Leib oder Leben eines ausländischen Staatsorgans und fällt damit unter die Straftaten von Gewicht, die eine behördliche Zusammenarbeit nahelegen.

78

2. Soweit das Antiterrordateigesetz als weitere Behörden den Bundesnachrichtendienst, den Militärischen Abschirmdienst, das Zollkriminalamt und die Bundespolizei einbezieht, ordnet Art. 73 Abs. 1 Nr. 1 und 5 GG die Gesetzgebungskompetenz dem Bund zu (vgl. BVerfGE 133, 277 <319 f. Rn. 100 ff.>).

79

Die Bundeskompetenz für die Einbeziehung des Bundesnachrichtendienstes ergibt sich aus der Zuständigkeit des Bundes für die Regelung der auswärtigen Beziehungen gemäß Art. 73 Abs. 1 Nr. 1 GG. Regelungen dafür müssen in einen Regelungs- und Verwendungszusammenhang eingebettet sein, der auf die Auslandsaufklärung bezogen ist (vgl. BVerfGE 100, 313 <370 f.>). Dabei kann der Bundesnachrichtendienst zwar nicht mit allgemeinen Befugnissen zur Verhütung, Verhinderung oder Verfolgung von Straftaten als solchen betraut werden, sondern nur mit Befugnissen von außen- und sicherheitspolitischer Bedeutung, die eine internationale Dimension aufweisen. Dies schließt jedoch ein, dass dem Bundesnachrichtendienst als eigene Aufgabe die Früherkennung solcher aus dem Ausland drohender Gefahren anvertraut werden kann, die sich ihrer Art und ihrem Gewicht nach auf die Stellung Deutschlands in der Staatengemeinschaft auswirken können und gerade in diesem Sinne von außen- und sicherheitspolitischer Bedeutung sind, wie etwa Gefahren durch staatenübergreifende Netzwerke der organisierten Kriminalität oder den Terrorismus (vgl. BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 128).

80

Hier eröffnet § 6a ATDG dem Bundesnachrichtendienst den Zugriff auf die in der Antiterrordatei gespeicherten Daten. Dieser ist aber nur für die Aufgaben der jeweils abfragenden Behörden eröffnet; dem Bundesnachrichtendienst werden damit also keine weiteren, allgemein auf die Verhinderung oder Verfolgung von Straftaten des internationalen Terrorismus gerichteten Befugnisse zugewiesen.

81

Hiermit vereinbar ist auch, dass der Bundesnachrichtendienst seine eigenen Daten durch Einstellung in die Datei anderer Behörden zugänglich macht. Denn das Antiterrordateigesetz begründet keine neuen, durch Art. 73 Abs. 1 Nr. 1 GG nicht mehr gedeckten Datenerhebungsbefugnisse, sondern knüpft an die für die eigene Aufgabenerfüllung erhobenen Daten an und verpflichtet lediglich dazu, diese Daten anderen Behörden für deren Aufgaben zugänglich zu machen. Die Regelung des Umfangs einer solchen zweckändernden Bereitstellung von Daten für andere Aufgabenträger ist kraft Sachzusammenhangs Teil der jeweiligen Kompetenz für die Datenerhebung und den damit korrespondierenden Datenschutz. Der Gesetzgeber gestaltet hierdurch den Bundesnachrichtendienst nicht in eine vorgelagerte Polizeibehörde um (vgl. BVerfGE 133, 277 <319 f. Rn. 101>). Entsprechend kann der Bund die Beteiligung des Militärischen Abschirmdienstes auf Art. 73 Abs. 1 Nr. 1 GG (Verteidigung) und der Bundespolizei sowie des Zollkriminalamts auf Art. 73 Abs. 1 Nr. 5 GG (Zoll- und Grenzschutz) stützen. Die Vorschriften tragen auch die Eröffnung eines Zugriffs dieser Behörden auf die Daten der Antiterrordatei (vgl. BVerfGE 133, 277 <320 Rn. 102>; hierzu auch BVerfGE 125, 260 <315>; 130, 151 <193>).

III.

Die erweiterte projektbezogene Datennutzung im Rahmen der Antiterrordatei genügt in ihrer konkreten Ausgestaltung jedoch in materieller Hinsicht teilweise nicht den Anforderungen aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Der damit verbundene Grundrechtseingriff in Gestalt der erweiterten Datennutzung durch Behörden, die diese Daten nicht selbst in die Datei eingestellt haben, steht mangels Regelung dafür erforderlicher Eingriffsschwellen in § 6a Abs. 2 ATDG mit dem Gebot der Verhältnismäßigkeit nicht in Einklang. Die angestrebte Eingrenzung der erweiterten Datennutzung durch ein Projekt im Sinne des § 6a Abs. 4 ATDG vermag die Verhältnismäßigkeit des Eingriffs in das Recht auf informationelle Selbstbestimmung nicht zu gewährleisten; die Bestimmungen der Absätze 6 bis 8 ändern daran nichts.

83

1. a) Eingriffe in das Recht auf informationelle Selbstbestimmung bedürfen wie jede Grundrechtsbeschränkung einer gesetzlichen Ermächtigung, die einen legitimen Gemeinwohlzweck verfolgt und im Übrigen den Grundsatz der Verhältnismäßigkeit wahrt (vgl. BVerfGE 65, 1 <44>; 100, 313 <359 f.>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 123 – Bestandsdatenauskunft II; stRspr). Sie müssen daher zur Erreichung des legitimen Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein (vgl. BVerfGE 141, 220 <265 Rn. 93>; stRspr). Dabei bedürfen sie einer gesetzlichen Grundlage, welche die Datenverwendung auf spezifische Zwecke hinreichend begrenzt (BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 123 – Bestandsdatenauskunft II).

84

b) Alle angegriffenen Befugnisse sind zudem am Grundsatz der Bestimmtheit und Normenklarheit zu messen, der der Vorhersehbarkeit von Eingriffen für die Bürgerinnen und Bürger, einer wirksamen Begrenzung der Befugnisse gegenüber der Ver-

85

waltung sowie der Ermöglichung einer effektiven Kontrolle durch die Gerichte dient (vgl. BVerfGE 113, 348 <375 ff.>; 120, 378 <407 f.>; 133, 277 <336 f. Rn. 140>; 141, 220 <265 Rn. 94>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 123 – Bestandsdatenauskunft II; vgl. auch EuGH, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 91; EGMR (GK), S. and Marper v. The United Kingdom, Urteil vom 4. Dezember 2008, Nr. 30562/04 u.a., § 99).

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 dabei gehalten, seine Regelungen so bestimmt zu fassen, wie dies nach der Eigenart des zu ordnenden Lebenssachverhalts mit Rücksicht auf den Normzweck möglich ist (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 Voraussetzungen 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>; 145, 20 <69 f. Rn. 125> m.w.N.). Dem Bestimmtheitserfordernis ist genügt, wenn die Auslegungsprobleme mit herkömmlichen juristischen Methoden bewältigt werden können (BVerfGE 134, 141 <184 f. Rn. 127> m.w.N.).

86

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>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 133 – Bestandsdatenauskunft II; jeweils m.w.N.; stRspr).

87

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. So hat die Rechtsprechung etwa lange und intransparente Verweisungsketten als Ver-

88

stoß gegen die Normenklarheit angesehen (vgl. BVerfGE 110, 33 <57, 62 f.>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 215).

c) Aus dem Verhältnismäßigkeitsprinzip folgen darüber hinaus im Bereich des Datenschutzes spezifische Anforderungen an Transparenz, Rechtsschutz und aufsichtliche Kontrolle (vgl. BVerfGE 125, 260 <344 ff.>; 150, 244 <285 Rn. 101>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 265; Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 203 – Bestandsdatenauskunft II; stRspr), welche sich im Einzelnen nach dem Eingriffsgewicht der Regelungen bemessen. Rechtsschutz und aufsichtliche Kontrolle können dabei die Einhaltung verhältnismäßiger Vorgaben nur sichern, nicht aber diese Vorgaben ersetzen. Verfassungsrechtlich geboten sind auch tragfähige Regelungen zur Nutzung der Daten sowie zur Datenlöschung (vgl. BVerfGE 65, 1 <46>; 150, 244 <285 Rn. 101>).

89

2. Die erweiterte Datennutzung nach § 6a ATDG verfolgt zwar ein legitimes Ziel (a) und ist hierfür geeignet und erforderlich (b). Den Anforderungen an die Angemessenheit hält § 6a Abs. 2 Satz 1 ATDG allerdings angesichts des erheblichen Gewichts des mit der erweiterten Datennutzung verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung nicht stand (c).

90

a) Die Antiterrordatei ist auf ein legitimes Ziel gerichtet (BVerfGE 133, 277 <321 Rn. 106>). Das gilt auch für die erweiterte Nutzung nach § 6a ATDG. Die Vorschrift zielt darauf ab, effektiv den Terrorismus zu bekämpfen (siehe dazu BTDrucks 18/1565, S. 19) und damit einhergehend den Bestand und die Sicherheit des Staates sowie Leib, Leben und Freiheit der Bevölkerung zu schützen (vgl. auch BVerfGE 133, 277 <321 Rn. 106, 333 f. Rn. 133>; 141, 220 <266 Rn. 96>). Straftaten mit dem Gepräge des Terrorismus zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Die Bereitstellung wirksamer Aufklärungsmittel zu ihrer Abwehr ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht (vgl. BVerfGE 115, 320 <357 f.>; 120, 274 <319>; 133, 277 <333 f. Rn. 133>; 141, 220 <266 Rn. 96> m.w.N.).

91

b) § 6a ATDG ist auch dazu geeignet, diesen Zweck zu fördern. Durch die Herstellung von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, den Ausschluss unbedeutender Informationen und Erkenntnisse, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie eine statistische Auswertung der in der Antiterrordatei gespeicherten Daten von Polizei und Nachrichtendiensten ermöglicht die erweiterte Datennutzung in § 6a ATDG die Herstellung vorher nicht bekannter Zusammenhänge zwischen verschiedenen in der Antiterrordatei gespeicherten Personen und deren Daten („Data-mining“), welche sowohl die Strafverfolgung und die Gefahrenabwehr als auch die wei-

92

tere nachrichtendienstliche Aufklärung entsprechender Strukturen erleichtern können.

Es mangelt auch nicht an der Erforderlichkeit der Regelung. Ein milderer Mittel, das gleich effektiv wäre, um solche Zusammenhänge herzustellen, ist weder vorgetragen noch ersichtlich. Die bloße Nutzung der Antiterrordatei als Indexdatei verlangsamt die Herstellung solcher Zusammenhänge nicht nur, sie dürfte sie im Regelfall sogar ganz verhindern, wenn zum Beispiel Kontaktpersonen getrennt von dem mutmaßlichen Gefährder gespeichert sind.

93

c) § 6a Abs. 2 Satz 1 ATDG genügt jedoch im Hinblick auf seine Angemessenheit den verfassungsrechtlichen Anforderungen nicht.

94

aa) Die Verhältnismäßigkeit im engeren Sinne verlangt insbesondere, dass die Einbußen an grundrechtlich geschützter Freiheit in keinem unangemessenen Verhältnis zu den Gemeinwohlzwecken stehen, denen eine Grundrechtsbeschränkung dient. Der Gesetzgeber muss zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herbeiführen. Dabei muss das Übermaßverbot gewahrt bleiben. Hierfür sind in einer Abwägung Reichweite und Gewicht des Eingriffs der Bedeutung der Regelung für eine wirksame staatliche Aufgabenwahrnehmung gegenüberzustellen. Im Hinblick auf die Verhältnismäßigkeit im engeren Sinne hat der Gesetzgeber die Ausgewogenheit zwischen der Art und Intensität der Grundrechtsbeeinträchtigung einerseits und den zum Eingriff berechtigenden Tatbestandselementen andererseits zu wahren; zu letzteren gehören die Eingriffsschwelle, die erforderliche Tatsachenbasis und das Gewicht der geschützten Rechtsgüter (vgl. BVerfGE 100, 313 <392 ff.>; 115, 320 <360>; 141, 220 <270 ff. Rn. 106 ff.>; 150, 244 <281 Rn. 91>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 130 m.w.N. – Bestandsdatenauskunft II; stRspr).

95

Das hierbei einzustellende Eingriffsgewicht wird vor allem durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt (vgl. BVerfGE 65, 1 <45 f.>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 129 – Bestandsdatenauskunft II). Dabei ist unter anderem bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben. Maßgebend sind also die Gestaltung der Eingriffsschwellen, die Zahl der Betroffenen und die Intensität der individuellen Beeinträchtigung im Übrigen. Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden (BVerfGE 115, 320 <347> m.w.N.). Dabei führt insbesondere die Heimlichkeit einer staatlichen Eingriffsmaßnahme ebenso zur Erhöhung ihrer Intensität (vgl. BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 129 m.w.N. – Bestandsdatenauskunft II) wie die

96

faktische Verwehrung vorherigen Rechtsschutzes und die Erschwerung nachträglichen Rechtsschutzes, wenn er überhaupt zu erlangen ist (vgl. BVerfGE 113, 348 <383 f.>; 118, 168 <197 f.>; 120, 378 <403>).

(1) Wird eine erweiterte Nutzung existierender Datenbestände durch eine Stelle zugelassen, die die Daten nicht selbst erhoben hat, so richtet sich die Verhältnismäßigkeit im engeren Sinne nach den Kriterien der hypothetischen Datenneuerhebung (vgl. BVerfGE 141, 220 <327 f. Rn. 287>).

97

(a) Erlaubt der Gesetzgeber die weitere Nutzung vorhandener Datenbestände, müssen die Verwendungsregelungen verhältnismäßig ausgestaltet sein. Der Gesetzgeber muss die Weiterverwendung an den Schutz hinreichend gewichtiger Rechtsgüter (vgl. BVerfGE 141, 220 <270 f. Rn. 106 ff.>; stRspr) und hinreichende Eingriffsschwellen (vgl. BVerfGE 141, 220 <271 ff. Rn. 109 ff.>; stRspr) binden (vgl. zuletzt BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 130 – Bestandsdatenauskunft II). Die Voraussetzungen für die Datenverwendung und deren Umfang in den betreffenden Rechtsgrundlagen müssen umso enger begrenzt werden, je schwerer der in der ersten Erhebung liegende Eingriff wiegt. Anlass, Zweck und Umfang des jeweiligen Eingriffs sowie die entsprechenden Eingriffsschwellen sind dabei durch den Gesetzgeber bereichsspezifisch, präzise bestimmt und normenklar zu regeln (vgl. BVerfGE 125, 260 <328>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 133 – Bestandsdatenauskunft II; jeweils m.w.N.).

98

Dabei hat der Gesetzgeber sicherzustellen, dass dem Eingriffsgewicht der Datenerhebung auch bei der Nutzung der Daten zu neuen Zwecken oder durch andere Stellen Rechnung getragen wird (vgl. BVerfGE 100, 313 <389 f.>; 109, 279 <377>; 120, 351 <369>; 130, 1 <33 f.>; 133, 277 <372 f. Rn. 225>; 141, 220 <326 f. Rn. 284>). Verfassungsrechtliche Voraussetzungen für die Erhebung, Speicherung und Verarbeitung von Daten dürfen nicht dadurch unterlaufen werden, dass Behörden, für die aufgrund ihrer Aufgabenstellung weniger strenge Anforderungen gelten, Daten im Wege der Übermittlung an Behörden weiterleiten, die ihrerseits strengeren Anforderungen unterliegen (BVerfGE 133, 277 <323 f. Rn. 114>). Maßgeblich ist insoweit nach dem Grundsatz der hypothetischen Datenneuerhebung, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck neu erhoben werden dürften (vgl. BVerfGE 125, 260 <333>; 133, 277 <373 ff. Rn. 225 f.>; 141, 220 <327 ff. Rn. 287 ff.>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 216).

99

Der Grundsatz der hypothetischen Datenneuerhebung gilt allerdings nicht schematisch abschließend und schließt die Berücksichtigung weiterer Gesichtspunkte nicht aus. So steht die Tatsache, dass die Zielbehörde einer Datenübermittlung bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, ihrerseits wegen ihres Aufgabenspektrums nicht vornehmen darf, einem Datenaustausch nicht prinzipiell entgegen. Auch können Gesichtspunkte der Vereinfachung und der Praktikabili-

100

tät bei der Schaffung von Übermittlungsvorschriften es rechtfertigen, dass nicht alle Einzelanforderungen, die für die Datenerhebung erforderlich sind, in gleicher Detailliertheit für die Übermittlung der Daten gelten. Das Erfordernis einer Gleichwertigkeit der neuen Nutzung bleibt hiervon jedoch unberührt (BVerfGE 141, 220 <327 f. Rn. 287> m.w.N.). Soweit Informationen nicht durch Wohnraumüberwachung oder den Zugriff auf informationstechnische Systeme erlangt wurden, müssen die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts nicht in jedem Fall identisch sein (vgl. BVerfGE 141, 220 <328 f. Rn. 289 und 291>).

(b) Regelungen, die den Austausch von Daten zwischen Polizeibehörden und Nachrichtendiensten ermöglichen, unterliegen dabei besonderen verfassungsrechtlichen Anforderungen (vgl. BVerfGE 133, 277 <329 Rn. 123>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17-, Rn. 218 f.; „informationelles Trennungsprinzip“). 101

(aa) Gesteigerte verfassungsrechtliche Anforderungen gelten für Vorschriften, welche die Nutzung nachrichtendienstlicher Informationen durch Polizei- und Sicherheitsbehörden ermöglichen. Die Aufgabe der Polizei- und Sicherheitsbehörden, Straftaten zu verhüten, zu verhindern und zu verfolgen sowie Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren, ist geprägt von einer operativen Verantwortung und der Befugnis, gegenüber Einzelnen Maßnahmen erforderlichenfalls auch mit Zwang durchzusetzen. Daher sind die Befugnisse hierzu eng und präzise zu fassen. Die Datenverarbeitung setzt grundsätzlich einen konkreten Anlass wie Anhaltspunkte für einen Tatverdacht oder eine Gefahr voraus (vgl. BVerfGE 133, 277 <327 f. Rn. 120>). 102

Demgegenüber dienen die Nachrichtendienste primär der Information der politischen Entscheidungsträger. Entsprechend dieser Aufgabe politischer Vorfeldaufklärung verfügen sie über weitreichende, nur an geringe Eingriffsschwellen geknüpfte Befugnisse zur Datensammlung (vgl. BVerfGE 133, 277 <325 f. Rn. 117>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 150 ff.). 103

Die Weite der Datenerhebungsbefugnisse der Nachrichtendienste wird grundsätzlich dadurch kompensiert, dass ihnen über die Aufgabe der Vorfeldaufklärung hinaus keine operative Verantwortung zukommt (vgl. BVerfGE 133, 277 <326 f. Rn. 118 f.>). Allerdings sind die Nachrichtendienste nicht notwendig auf die politische Vorfeldaufklärung beschränkt. So übernimmt der Bundesnachrichtendienst als eigene Aufgabe vermehrt auch die Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Dimension (vgl. BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 128) und die Weiterleitung von Informationen aus der Gefahrenfrüherkennung an Polizei- und Sicherheitsbehörden (vgl. §§ 24 f. BNDG; § 19 BVerfSchG; § 11 MADG). Dadurch mag sich der Abstand zwischen Nachrichtendiensten und Polizeibehörden verringern (vgl. Schwabenbauer, Heimliche Grundrechtseingriffe, 2013, S. 17 ff.). Das ändert aber nichts daran, dass den Nachrichten- 104

diensten für die Gefahrenfrüherkennung vergleichbar weitreichende Befugnisse zur Datensammlung zur Verfügung stehen wie bei der politischen Vorfeldaufklärung und dass sie im Gegenzug nicht operativ tätig werden.

Die Unterschiede bei der Aufgabenstellung und die daraus folgende Gefahr des Unterlaufens spezifischer Anforderungen an die Sammlung und Verwertung von Daten bedingen gesteigerte verfassungsrechtliche Anforderungen an Vorschriften, welche die Nutzung nachrichtendienstlicher Informationen durch Polizei- und Sicherheitsbehörden ermöglichen. Das entspricht dem Erfordernis eines herausragenden öffentlichen Interesses und hinreichend konkreter und qualifizierter Übermittlungsschwellen (vgl. BVerfGE 133, 277 <329 Rn. 123>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 218 f.).

(bb) Anderes gilt für die Nutzung der Daten von Polizei- und Sicherheitsbehörden durch die Nachrichtendienste. Diese Daten wurden bereits nach den strengeren Anforderungen erhoben, die für operativ tätige Behörden mit der Befugnis zu Zwangsmaßnahmen gegenüber Einzelnen gelten. Diese Anforderungen können also durch eine Nutzung der Daten durch Nachrichtendienste nicht unterlaufen werden. Zudem können diese Daten von den mit der Aufgabe der Vorfeldaufklärung betrauten Nachrichtendiensten nicht operativ für Zwangsmaßnahmen gegenüber Einzelnen verwendet werden (zu den sich daraus ergebenden Anforderungen unten Rn. 119).

(2) Welche Anforderungen nach dem Grundsatz der hypothetischen Datenneuerhebung an die Ausgestaltung einer Befugnis hinsichtlich Rechtsgüterschutz und Eingriffsschwelle im Einzelnen zu stellen sind, richtet sich nach der konkreten Belastungswirkung. Die erweiterte Nutzung einer Verbunddatei gemeinsam durch Nachrichtendienste und Polizeibehörden nach § 6a Abs. 5 ATDG hat, insbesondere im Vergleich zur einfachen Nutzung nach § 5 ATDG (vgl. dazu BVerfGE 133, 277 <322 ff. Rn. 110 ff.>), gesteigerte Belastungswirkung.

(a) Wie schon bei der einfachen Nutzung einer Verbunddatei, wie sie § 5 ATDG vorsieht, entsteht die Belastung zunächst dadurch, dass Polizei- und Sicherheitsbehörden Zugriff auf von den Nachrichtendiensten gewonnene Daten erhalten. Die Befugnis zur erweiterten Nutzung von Daten durch Polizei- und Sicherheitsbehörden nach § 6a Abs. 2 und 3 ATDG umfasst – mit Ausnahme der nach § 4 ATDG verdeckt gespeicherten Daten – alle in die Antiterrordatei eingespeicherten Datenarten nach § 3 ATDG und damit auch Daten, die die Nachrichtendienste mit den ihnen zur Verfügung stehenden Instrumenten der Vorfeldaufklärung erhoben haben. Daher gelten zur Vermeidung des Unterlaufens der den Polizei- und Sicherheitsbehörden vorgegebenen qualifizierten Eingriffsschwellen insoweit gesteigerte verfassungsrechtliche Anforderungen für die erweiterte Nutzung durch diese Behörden.

(b) Das Eingriffsgewicht wird zudem sowohl bei der Nutzung durch Polizei- und Sicherheitsbehörden als auch bei der Nutzung durch Nachrichtendienste durch das so ermöglichte „Data-mining“ erhöht. Werden in einer Datei gespeicherte Daten aus verschiedenen nachrichtendienstlichen und polizeilichen Quellen im Wege der Verknüp-

fung zur Erzeugung neuer Erkenntnisse und Zusammenhänge genutzt (erweiterte Nutzung), so kommt dem grundsätzlich eine gesteigerte Belastungswirkung zu.

(aa) Das Eingriffsgewicht der Antiterrordatei war ursprünglich dadurch gemindert, dass sie als Verbunddatei in ihrem Kern auf die Informationsanbahnung beschränkt war und eine Nutzung der Daten zur operativen Aufgabenwahrnehmung nur in dringenden Ausnahmefällen vorsah (vgl. BVerfGE 133, 277 <329 Rn. 124>). Demgegenüber ermöglicht eine erweiterte projektbezogene Nutzung, wie sie nunmehr § 6a Abs. 5 ATDG beschreibt und die von allen an der Antiterrordatei beteiligten Behörden heimlich durchgeführt wird, nicht nur eine Informationsanbahnung nach Maßgabe des Fachrechts, sondern als Ergebnis einer automatisierten Verknüpfung und Analyse der von verschiedenen Behörden in die Antiterrordatei eingespeisten Daten auch die Erzeugung neuer Erkenntnisse und Zusammenhänge („Data-mining“), die eine erhebliche Persönlichkeitsrelevanz aufweisen können (vgl. zur Rasterfahndung BVerfGE 115, 320 <350 f.>).

110

Soweit solche neuen Erkenntnisse und Zusammenhänge gemäß § 6a Abs. 2 und 3 ATDG von Polizei- und Sicherheitsbehörden generiert werden, wird das Eingriffsgewicht dadurch weiter erhöht, dass diese neuen Erkenntnisse unmittelbar zu operativen Zwecken verwendet werden können.

111

(bb) Letzteres ist nicht der Fall, wenn die selbst nicht operativ tätigen Nachrichtendienste die Antiterrordatei nach § 6a Abs. 1 ATDG für das „Data-mining“ nutzen. Insofern fließen die neu erzeugten Erkenntnisse lediglich in die weitere Vorfeldaufklärung ein. Aber auch hier ist zu berücksichtigen, dass die Nachrichtendienste selbst im Wege der erweiterten Nutzung neue Erkenntnisse und Zusammenhänge von möglicherweise erheblicher Persönlichkeitsrelevanz erzeugen können (vgl. zur Rasterfahndung BVerfGE 115, 320 <350 f.>). Dies könnte ein Gefühl des unkontrollierbaren Beobachtetwerdens hervorrufen und nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung entfalten (vgl. BVerfGE 125, 260 <332>), weil, ohne dass die Einzelnen davon Kenntnis erlangen, in den Dateien gespeicherte Daten verschiedenen Ursprungs und Gewichts zu verschiedenen Zwecken kombiniert werden können.

112

(cc) Gemindert wird das Eingriffsgewicht allerdings insoweit, als die Nachrichtendienste und Sicherheitsbehörden durch die erweiterte Datennutzung gemäß § 6a Abs. 1 bis 3 in Verbindung mit § 4 Abs. 3 ATDG nicht auf verdeckt gespeicherte Daten zurückgreifen können, die durch die besonders gewichtigen Eingriffe in das Telekommunikationsgeheimnis oder das Grundrecht auf Unverletzlichkeit der Wohnung (insbesondere durch Telekommunikations- oder Wohnraumüberwachung) sowie in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG (wie bei der Online-Durchsuchung) gewonnen wurden. Solche Daten können regelmäßig nur unter strengen Maßgaben erhoben werden (vgl. BVerfGE 133, 277 <372 ff. Rn. 224 ff.> m.w.N.).

113

Auch wenn diese sogenannten verdeckten Daten (§ 4 ATDG) bei der erweiterten Nutzung außen vor bleiben, sind die in der Datei nach § 3 ATDG gespeicherten Daten, insbesondere die erweiterten Grunddaten im Sinne des § 3 Abs. 1 Nr. 1 Buchstabe b ATDG, allerdings von erheblicher Bedeutung. Der Informationsgehalt der erweiterten Grunddaten gemäß § 3 Abs. 1 Nr. 1 Buchstabe b ATDG reicht inhaltlich weit und kann höchstpersönliche sowie die Biographie der Betroffenen nachzeichnende Informationen enthalten (BVerfGE 133, 277 <363 f. Rn. 199>). 114

(3) Nach der so bestimmten Belastungswirkung bemessen sich nun dem Grundsatz der hypothetischen Datenneuerhebung gemäß die konkreten Anforderungen an die Rechtsgüter und die Eingriffsschwellen. 115

(a) Bei diesem Eingriffsgewicht muss die Erzeugung neuer Erkenntnisse und Zusammenhänge durch Verknüpfung von in einer Datei gespeicherten Daten aus verschiedenen nachrichtendienstlichen und polizeilichen Quellen einem herausragenden öffentlichen Interesse dienen (vgl. BVerfGE 133, 277 <329 Rn. 123>) und ist daher nur zum Schutz von besonders gewichtigen Rechtsgütern wie Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes zulässig (vgl. auch BVerfGE 133, 277 <365 Rn. 203>; 141, 220 <270 f. Rn. 108; 328 ff. Rn. 288, 292>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 221). 116

(b) Der Eingriff durch erweiterte Nutzung muss an hinreichend konkretisierte Eingriffsschwellen für die erweiterte Nutzung zu Zwecken der Gefahrenabwehr, Strafverfolgung sowie der Aufgabenerfüllung von nicht operativ tätig werdenden Behörden wie den Nachrichtendiensten auf der Grundlage normenklarer Regelungen gebunden sein (vgl. BVerfGE 133, 277 <329 Rn. 123>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 197 – Bestandsdatenauskunft II). 117

(aa) Für die erweiterte Nutzung der Antiterrordatei zum Zwecke der Gefahrenabwehr muss wegen der beschriebenen Belastungswirkung eine wenigstens hinreichend konkretisierte Gefahr in dem Sinne gegeben sein, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr vorliegen (vgl. BVerfGE 141, 220 <271 f. Rn. 111 f.>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 222; zu den weniger strengen Anforderungen für den einfachen Zugriff nach § 5 Abs. 1 ATDG vgl. BVerfGE 133, 277 <360 ff. Rn. 193 ff.>). Soweit wie bei terroristischen Straftaten besonders gewichtige Rechtsgüter wie Leib, Leben, Freiheit der Person, Bestand oder Sicherheit des Bundes oder eines Landes betroffen sind, ist die konkretisierte Gefahr als Eingriffsschwelle allerdings auch ausreichend (vgl. BVerfGE 141, 220 <270 f. Rn. 108, 272 f. Rn. 112>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 147 f. – Bestandsdatenauskunft II; vgl. bereits BVerfGE 115, 320 <364 f.> zur Rasterfahndung). 118

(bb) Diese verfassungsrechtlichen Anforderungen gelten grundsätzlich für alle Ein- 119

griffsermächtigungen mit präventiver Zielrichtung, also auch für die Verwendung dieser Daten durch Nachrichtendienste. Auch für ihre Tätigkeiten sind insoweit tatsächliche Anhaltspunkte erforderlich (zu den Besonderheiten der nachrichtendienstlichen Ausland-Ausland-Fernmeldeaufklärung vgl. jedoch BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 155 ff.). Bei nicht tief in die Privatsphäre eingreifenden und insgesamt weniger gewichtigen Eingriffen kann es jedoch genügen, dass eine Auskunft zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist, denn damit wird ein wenigstens der Art nach konkretisiertes und absehbares Geschehen vorausgesetzt (vgl. BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 151 m.w.N. – Bestandsdatenauskunft II). Diese zur Bestandsdatenauskunft formulierten Maßstäbe gelten auch für die erweiterte Nutzung der Antiterrordatei durch Nachrichtendienste. Zum einen haben diese von vornherein die Aufgabe, besonders gewichtige Rechtsgüter zu schützen (vgl. BVerfGE 141, 220 <339 f. Rn. 320>; vgl. auch BVerfGE 133, 277 <326 Rn. 118>). Zum anderen handelt es sich zwar hier nicht um „nicht tief in die Privatsphäre eingreifende und insgesamt weniger gewichtige“ Eingriffe (zum Eingriffsgewicht der erweiterten Nutzung oben Rn. 109 ff.). Maßgeblich ist hier indessen, dass bei deren ersten Erhebung durch die Polizeibehörden bereits die Eingriffsschwelle für die operativen Tätigkeiten der Polizei überschritten werden musste und diese nicht auch für die weitere Nutzung der erhobenen Daten gilt (vgl. insoweit BVerfGE 141, 220 <328 f. Rn. 289>).

(cc) Für die erweiterte Nutzung von Daten zur Strafverfolgung genügen die Anforderungen nicht, die § 152 Abs. 2 StPO an die Einleitung eines Ermittlungsverfahrens stellt (zureichende tatsächliche Anhaltspunkte). Der Gesetzgeber muss als Eingriffsschwelle vielmehr festlegen, dass bestimmte, den Verdacht begründende Tatsachen vorliegen müssen. Das bedeutet, dass insoweit konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorhanden sein müssen (vgl. BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 222 m.w.N.).

bb) Diesen differenzierten Anforderungen wird § 6a ATDG nicht in vollem Umfang gerecht. Zwar entspricht § 6a ATDG den hier zu wählenden Anforderungen an den Rechtsgüterschutz, da er die erweiterte Nutzung nur zum Schutz von Rechtsgütern zulässt, die besonders gewichtig sind wie Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes. Der Befugnis nach § 6a Abs. 2 Satz 1 ATDG fehlt jedoch eine hinreichend qualifizierte Eingriffsschwelle.

Den verfassungsrechtlichen Anforderungen hat der Gesetzgeber dadurch Rechnung zu tragen gesucht, dass er für Datenverknüpfung und „Data-mining“ in einzel-fallbezogenen Projekten zur Sammlung und Auswertung von Informationen, zur Strafverfolgung und zur Gefahrenabwehr unterschiedliche Regelungen zur Aufklärung und Bekämpfung des internationalen Terrorismus vorgesehen hat (§ 6a Abs. 1, 2 und 3 ATDG). Zwar stellen die Aufklärung und Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland (§ 1 Abs. 1 ATDG) ein her-

ausragendes öffentliches Interesse dar (oben Rn. 91). Das Fehlen hinreichend qualifizierter Eingriffsschwellen in § 6a Abs. 2 ATDG verstößt jedoch gegen das Übermaßverbot. Die erweiterte Datennutzung ist insoweit auch mit der Bindung an ein Projekt im Sinne von § 6a Abs. 4 ATDG nicht mit den erforderlichen Eingriffsschwellen versehen. Der für die Nutzung zum Zwecke der Strafverfolgung (§ 6a Abs. 2 ATDG) gebotene verdichtete Tatverdacht wird nicht normenklar festgelegt. Auch die Bestimmungen zu Aufsicht (§ 6a Abs. 7 ATDG) und Rechtskontrolle (§ 6a Abs. 8 ATDG) können materielle Anforderungen nicht ersetzen.

(1) § 6a Abs. 1 ATDG erweist sich allerdings insoweit als verfassungsgemäß, als er unter bestimmten Voraussetzungen, die im Einklang mit den verfassungsrechtlichen Anforderungen auszulegen sind, Behörden des Bundes, insbesondere Nachrichtendiensten, den Zugriff auf die nicht verdeckt gespeicherten Daten der Antiterrordatei zur Sammlung und Auswertung von Informationen über eine internationale terroristische Bestrebung erlaubt. Die Vorschrift regelt noch hinreichend bestimmt und normenklar, dass sie nur auf Behörden anwendbar ist, soweit diese Informationen sammeln, jedoch nicht selbst operativ tätig sind, also insbesondere Nachrichtendienste, aber auch etwa das Bundeskriminalamt als Zentralstelle (§ 2 BKAG) ([a]). Sie enthält auch eine hinreichende Regelung der konkreten Eingriffsschwelle ([b]).

(a) Der Anwendungsbereich von § 6a Abs. 1 ATDG erfasst – neben der Öffnung der Daten für eine Verwendung durch berechtigte Landesbehörden (vgl. § 6a Abs. 11 ATDG) – sämtliche „beteiligte Behörden des Bundes“ gemäß § 1 ATDG, sofern diese „zur Erfüllung ihrer gesetzlichen Aufgaben“ handeln. Entsprechend der Zwecksetzung des Projekts muss die Aufgabe, zu deren Erfüllung die Nutzung der Antiterrordatei erforderlich sein soll, in der „Sammlung und Auswertung von Informationen“ über eine internationale terroristische Bestrebung bestehen. Dies trifft vornehmlich auf Nachrichtendienste zu, deren Aufgabe in erster Linie in der Sammlung, Auswertung und Weitergabe von Informationen besteht. Eine Beschränkung auf Nachrichtendienste enthält die Vorschrift jedoch nicht.

In Reaktion auf die Kritik an der Bestimmtheit des Entwurfs der Bundesregierung wurden die „bislang im Absatz 1 des Entwurfs zusammengefassten drei Fallgruppen auf drei Absätze aufgeteilt“ (BTDrucks 18/2902, S. 12; vgl. auch Evaluierung des Rechtsextremismus-Datei-Gesetzes, BTDrucks 18/8060, S. 113, 119). Eine klarstellende Beschränkung von Absatz 1 auf Nachrichtendienste erfolgte aber nicht. § 6a Abs. 1 ATDG erfasst somit etwa auch das Bundeskriminalamt, soweit es als Zentralstelle für den polizeilichen Informationsverbund befugt ist, zur Unterstützung der Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung, alle hierfür erforderlichen Informationen zu sammeln und auszuwerten (§ 2 Abs. 1, Abs. 2 Nr. 1, §§ 29 ff. BKAG). Allerdings muss die Aufgabe, zu deren Erfüllung die Nutzung der Antiterrordatei erforderlich sein soll, nach dem Gesetzeswortlaut in der „Sammlung und Auswertung von Informationen“ über eine internationale terroristische Bestrebung bestehen. Es darf sich nicht um eine operative Aufgabe handeln. Das ergibt

sich aus der Systematik des § 6a ATDG, welcher zwischen erweiterter Nutzung zur Informationssammlung und -auswertung (Absatz 1), zur Strafverfolgung (Absatz 2) und zur Gefahrenabwehr (Absatz 3) unterscheidet. Die erweiterte Nutzung zum Zwecke der Strafverfolgung und zur Gefahrenabwehr richtet sich nicht nach § 6a Abs. 1 ATDG, sondern nach § 6a Abs. 2 und 3 ATDG. Dies schließt also eine erweiterte Nutzung im Rahmen von Befugnissen zur Strafverfolgung und zur Abwehr von Gefahren des internationalen Terrorismus auf der Grundlage von Absatz 1 aus.

(b) Der Bestimmung in § 6a Abs. 1 ATDG ist im Wege der Auslegung eine hinreichend normenklar geregelte Eingriffsschwelle zu entnehmen, welche den verfassungsrechtlichen Anforderungen (oben Rn. 118 f.) genügt. § 6a Abs. 1 ATDG verlangt, dass die erweiterte Nutzung im Sinne von § 6a Abs. 5 ATDG im Einzelfall zur Sammlung und Auswertung von Informationen über eine internationale terroristische Bestrebung durch die Nachrichtendienste erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass Straftaten des internationalen Terrorismus nach den §§ 129a, 129b und 211 StGB begangen werden sollen und dadurch Gefahren für Leib, Leben oder Freiheit von Personen drohen. Insoweit ergibt sich aus dem Erfordernis der Erforderlichkeit der Aufklärung weiterer Zusammenhänge des Einzelfalls, dass eine Nutzung zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss (vgl. dazu BVerfGE 130, 151 <206>). Darin ist das erforderliche Merkmal der Gebotenheit im Einzelfall enthalten. Das genügt den Anforderungen an eine Eingriffsschwelle für das bloße Sammeln und Auswerten von Informationen ohne operative Komponente (vgl. oben Rn. 118); soweit neben den Nachrichtendiensten auch andere Behörden nicht operativ tätig werden, gilt dies entsprechend.

126

(2) In der Regelung des § 6a Abs. 2 Satz 1 ATDG fehlen hingegen die erforderlichen Eingriffs- beziehungsweise Verdachtsschwellen. § 6a Abs. 2 ATDG dient der Erfüllung repressiver Aufgaben. In den Anwendungsbereich fallen damit klassischerweise die beteiligten Strafverfolgungsbehörden, nicht jedoch die Nachrichtendienste. Die Möglichkeit der erweiterten Nutzung von Daten, die seitens der Nachrichtendienste in die Antiterrordatei eingestellt wurden, durch die Strafverfolgungsbehörden führt dazu, dass qualifizierte Eingriffsschwellen erforderlich sind (vgl. oben Rn. 120). Es bedarf bestimmter den Verdacht begründender Tatsachen. Daran fehlt es bei § 6a Abs. 2 ATDG.

127

§ 6a Abs. 2 Satz 1 ATDG fordert für die erweiterte Nutzung hinsichtlich der qualifizierten Straftaten keinerlei begründeten Verdacht, sondern lässt die „Erforderlichkeit im Einzelfall“ zur Aufklärung „weitere[r] Zusammenhänge des Einzelfalls“ genügen. Aus dem gesetzlichen Tatbestandsmerkmal der Erforderlichkeit im Einzelfall könnte hier zwar möglicherweise gefolgert werden, dass zumindest ein Anfangsverdacht im Sinne von § 152 Abs. 2 StPO vorliegen muss (vgl. dazu BVerfGE 130, 151 <206>). Doch auch dies genügte als Eingriffsschwelle für eine erweiterte Datennutzung zum Zwecke der Strafverfolgung nicht. § 6a Abs. 2 ATDG bestimmt nicht in der gebotenen

128

normenklaren Weise, dass es eines vom strafprozessualen Anfangsverdacht verschiedenen verdichteten Tatverdachts (oben Rn. 120) bedarf. Das gilt trotz der Bindung an ein Projekt nach § 6a Abs. 4 ATDG (näher unten Rn. 132 ff.).

(3) § 6a Abs. 3 ATDG erweist sich bei einer Auslegung am Maßstab der Verfassung im Ergebnis als verhältnismäßig. Die Vorschrift richtet sich an beteiligte Polizeibehörden, denen die erweiterte Nutzung von Daten, die unter anderem seitens der Nachrichtendienste in die Antiterrordatei eingestellt wurden, mit dem Ziel der Verhinderung von qualifizierten Straftaten des internationalen Terrorismus ermöglicht wird. Auch insofern bedarf es qualifizierter Eingriffsschwellen. Dafür muss eine wenigstens hinreichend konkretisierte Gefahr gegeben sein (oben Rn. 118). 129

§ 6a Abs. 3 ATDG ermächtigt die Behörden zur erweiterten Nutzung der Antiterrordatei für die Verhinderung von qualifizierten Straftaten des internationalen Terrorismus, wenn Tatsachen die Annahme rechtfertigen, dass eine solche Straftat begangen werden soll. Den Anforderungen an das Vorliegen einer konkretisierten Gefahr genügt es nicht, wenn das Gesetz allein verlangt, dass Tatsachen vorliegen, die die Annahme rechtfertigen, dass eine Straftat begangen werden soll, weil dies nicht ausschließt, dass sich die behördliche Prognose allein auf Erfahrungssätze stützt (vgl. BVerfGE 141, 220 <291 Rn. 165>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 225 f. – Bestandsdatenauskunft II). Die Befugnis nach § 6a Abs. 3 ATDG ist jedoch insofern enger gefasst, als die erweiterte Nutzung der Antiterrordatei dafür erforderlich sein muss, weitere Zusammenhänge des Einzelfalls aufzuklären. Letzteres muss bei durch den Grundsatz der Normenklarheit nicht ausgeschlossener verfassungskonformer Auslegung von § 6a Abs. 3 ATDG so verstanden werden, dass eine weitere Nutzung der Datei erst zulässig ist, wenn die Behörde bereits ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennt oder erkennt, dass das individualisierte Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in absehbarer Zeit terroristische Straftaten begeht (vgl. BVerfGE 141, 220 <272 f. Rn. 112, 290 f. Rn. 164>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 226 – Bestandsdatenauskunft II). Die erweiterte Nutzung setzt demnach eine solchermaßen konkretisierte Gefahr voraus, zu deren weiterer Aufklärung sie, was hinreichend klar erkennbar ist, dienen muss. 130

Dabei darf das gesetzliche Tatbestandsmerkmal „um weitere Zusammenhänge des Einzelfalls aufzuklären“ nicht so verstanden werden, als erlaubte die Bestimmung die erweiterte Nutzung für eine bloße Vor- oder Umfeldermittlung ohne Bezug zu einer zumindest konkretisierten Gefahr (dazu oben Rn. 118). Bei einer solchen Lesart wäre § 6a Abs. 3 ATDG verfassungswidrig. 131

(4) Auch die Bindung an ein Projekt im Sinne des § 6a Abs. 4 ATDG ändert nichts an der verfassungsrechtlichen Unzulänglichkeit der in § 6a Abs. 2 ATDG genannten Eingriffsvoraussetzungen. 132

(a) Nach § 6a Abs. 4 ATDG ist ein Projekt eine gegenständlich abgrenzbare und auf 133

bestimmte Zeiträume bezogene Aufgabe, der durch die Gefahr oder den drohenden Schaden, die am Sachverhalt beteiligten Personen, die Zielsetzung der Aufgabe oder deren Folgewirkungen eine besondere Bedeutung zukommt. Diese Legaldefinition in § 6a Abs. 4 ATDG verdeutlicht das berechnete Anliegen des Gesetzgebers, durch eine offene Projektdefinition den beteiligten Akteuren einen weiten Handlungsspielraum einzuräumen, um den Kampf gegen den internationalen Terrorismus effektiv betreiben und auch auf Veränderungen, Unerwartetes und Unsicherheiten reagieren zu können. Dies entbindet ihn aber nicht von den verfassungsrechtlichen Anforderungen an eine Festlegung von hinreichenden Eingriffsschwellen für die in Absatz 2 geregelten Befugnisse. Die Einrichtung eines Projekts ist in Absatz 4 ebenfalls nicht an eine Eingriffsschwelle gebunden.

(b) Das Fehlen einer hinreichenden Eingriffsschwelle ist auch nicht wegen der persönlichen und zeitlichen Eingrenzung in § 6a Abs. 6 Satz 2 ATDG auf insgesamt vier Jahre verfassungsrechtlich unbedenklich. 134

(5) Die in § 6a Abs. 7 und 8 ATDG normierten Anforderungen an individuellen Rechtsschutz und aufsichtliche Kontrolle genügen den aus dem Verhältnismäßigkeitsgrundsatz im Bereich der informationellen Selbstbestimmung folgenden Maßgaben (vgl. BVerfGE 133, 277 <365 ff. Rn. 204 ff.> m.w.N.). Dabei ergänzen sich administrative und gerichtsähnliche Rechtskontrolle (vgl. BVerfGE 133, 277 <369 Rn. 213>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 274). Hier erscheint eine vorherige Rechtskontrolle allerdings insbesondere in Eilfällen nicht unbedingt erforderlich (vgl. BVerfGE 133, 277 <369 Rn. 213>; BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 254 – Bestandsdatenauskunft II). Daher stößt das differenzierte Kontrollverfahren, das eine aufsichtliche (Absatz 7) und eine grundsätzlich vorherige Rechtskontrolle durch die G 10-Kommission (Absatz 8) verbindet, die bei Gefahr im Verzug nachgeholt werden kann, nicht auf verfassungsrechtliche Bedenken. Die bloße Kontrolle kann allerdings das Fehlen einschränkender materieller Kriterien für die erweiterte Datennutzung nach § 6a Abs. 2 ATDG nicht ersetzen, da die Einhaltung der Grenzen des Projekts und der Eingriffsbefugnisse nur anhand materieller Bestimmungen kontrolliert werden kann (vgl. dazu auch BVerfGE 110, 33 <67 f.>; 120, 274 <331>). 135

D.

I.

Demnach verstößt § 6a Abs. 2 Satz 1 ATDG gegen das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Der Verstoß einer Norm gegen das Grundgesetz hat im Grundsatz deren Nichtigkeit zur Folge (§ 95 Abs. 3 BVerfGG; vgl. BVerfGE 65, 325 <357>; 114, 316 <338>). Ausnahmsweise kann das Bundesverfassungsgericht ihre Unvereinbarkeit mit dem Grundgesetz (Verfassungswidrigkeit) feststellen (vgl. § 31 Abs. 2 Satz 2, § 79 Abs. 1 136

BVerfGG). Gründe, warum die Norm einstweilen fortgelten sollte, sind hier allerdings nicht ersichtlich.

II.

Die Auslagenerstattung beruht auf § 34a Abs. 2 BVerfGG. 137

III.

Gemäß § 4 Abs. 4, § 15 Abs. 3 Satz 1 BVerfGG hat der Erste Senat in der Besetzung von sieben Richterinnen und Richtern entschieden. 138

Harbarth

Paulus

Baer

Britz

Ott

Christ

Radtke

**Bundesverfassungsgericht, Beschluss des Ersten Senats vom 10. November 2020 -
1 BvR 3214/15**

Zitiervorschlag BVerfG, Beschluss des Ersten Senats vom 10. November 2020 -
1 BvR 3214/15 - Rn. (1 - 138), [http://www.bverfg.de/e/
rs20201110_1bvr321415.html](http://www.bverfg.de/e/rs20201110_1bvr321415.html)

ECLI ECLI:DE:BVerfG:2020:rs20201110.1bvr321415