

Stellungnahme des Bundesrates

Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus

Der Bundesrat hat in seiner 946. Sitzung am 17. Juni 2016 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zu Artikel 1 Nummer 2 (§ 22b Absatz 1 BVerfSchG)

In Artikel 1 Nummer 2 § 22b Absatz 1 sind die Wörter "Erforschung von Bestrebungen oder Tätigkeiten, die sich auf bestimmte Ereignisse oder Personenkreise beziehen," durch die Wörter "Erfüllung seiner gesetzlichen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland," zu ersetzen.

Begründung:

Die Zweckbestimmung in § 22b Absatz 1 BVerfSchG-E ("zur Erforschung von Bestrebungen oder Tätigkeiten, die sich auf bestimmte Ereignisse oder Personenkreise beziehen") ist nicht geeignet, die Bestimmtheit der Ermächtigungsgrundlage zu erhöhen. Gemäß § 4 Absatz 1 Satz 3 BVerfSchG setzt die Sammlung und Auswertung von Informationen durch das Bundesamt für Verfassungsschutz das Vorliegen tatsächlicher Anhaltspunkte für Bestrebungen oder Tätigkeiten im Sinne von § 3 Absatz 1 BVerfSchG voraus. Unabhängig von der Art und Weise der Informationsbeschaffung muss sich also die Tätigkeit des Bundesamts für Verfassungsschutz stets auf bestimmte Bestrebungen und Tätigkeiten beziehen. Auch die zur Konkretisierung herangezogenen "Ereignisse" und "Personenkreise" laufen letztlich auf eine Tautologie hinaus. Denn der Begriff "Bestrebungen" ist in § 4 Absatz 1 Satz 1 BVerfSchG schon legaldefiniert als "Verhaltensweisen in einem oder für einen Personenzusammenschluss".

Aus gesamtsystematischer Sicht überzeugt es zudem nicht, wenn für gemeinsame Dateien zur Bekämpfung des internationalen Terrorismus, an denen ausländische Nachrichtendienste beteiligt sind, eine andere Terminologie verwendet wird als bei der auf inländische Behörden beschränkten Antiterrordatei (vgl. § 1 Absatz 1 ATDG: "zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland").

Die Formulierung sollte daher an § 1 Absatz 1 ATDG angelehnt werden.

2. Zu Artikel 1 Nummer 2 (§ 22b Absatz 1 Nummer 2 BVerfSchG)

In Artikel 1 Nummer 2 sind in § 22b Absatz 1 Nummer 2 die Wörter "gewährleistet ist," durch die Wörter "sowie gewährleistet ist, dass die Nutzung der Daten in den teilnehmenden Staaten weder zu politischer Verfolgung noch unmenschlicher oder erniedrigender Bestrafung oder Behandlung verwendet werden," zu ersetzen.

Begründung:

Soweit der Gesetzentwurf bislang allein die Einhaltung grundlegender rechtsstaatlicher Prinzipien durch die teilnehmenden Staaten verlangt, genügt dies nicht den Anforderungen, die das Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 (1 BvR 966/09) für die Übermittlung personenbezogener Daten an ausländische Stellen aufgestellt hat. Es hat in diesem Urteil insoweit ausgeführt:

"Hinsichtlich der Besorgnis etwaiger Menschenrechtsverletzungen durch die Nutzung der Daten im Empfängerstaat muss insbesondere gewährleistet erscheinen, dass sie dort weder zu politischer Verfolgung noch unmenschlicher oder erniedrigender Bestrafung oder Behandlung verwendet werden (vgl. Artikel 16a Absatz 3 GG). Der Gesetzgeber hat insgesamt Sorge zu tragen, dass der Schutz der Europäischen Menschenrechtskonvention und der anderen internationalen Menschenrechtsverträge (vgl. Artikel 1 Absatz 2 GG) durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen nicht ausgehöhlt wird." (vgl. BVerfG, am angegebenen Ort, Rn. 336).

Dieser Vorgabe wird durch den Gesetzentwurf nicht vollständig entsprochen, weil es auch in Staaten, in denen "grundlegende rechtsstaatliche Prinzipien" eingehalten werden, in Folge der Nutzung der übermittelten Daten etwa zu politischer Verfolgung oder unmenschlicher Behandlung oder Bestrafung kommen kann. Dies ist etwa dann der Fall, wenn die Datennutzung zur Verhängung und Vollstreckung der Todesstrafe führen kann. Jedenfalls die Situation vor der Hinrichtung stellt nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte eine Verursachung erheblicher psychischer Leiden und somit eine unmenschliche Behandlung im Sinne von Artikel 3 EMRK dar (vgl. Urteil vom 7. Juli 1989, Soering/Vereinigtes Königreich EGMR-E 4, 376 ff.).

Vor diesem Hintergrund ist mit der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen, dass die Errichtung gemeinsamer Dateien nur mit solchen Staaten in Betracht kommen, welche die Gewähr dafür bieten, dass sie die übermittelten Daten weder zu politischer Verfolgung noch unmenschlicher oder erniedrigender Bestrafung oder Behandlung verwenden.

3. Zu Artikel 1 Nummer 2 (§ 22b Absatz 1 Satz 2 - neu - BVerfSchG)

In Artikel 1 Nummer 2 ist dem § 22b Absatz 1 folgender Satz anzufügen:

"Das Vorliegen der Voraussetzungen gemäß Satz 1 ist vom Bundesamt für Verfassungsschutz schriftlich zu dokumentieren."

Begründung:

§ 22b Absatz 1 BVerfSchG-E statuiert in Satz 1 Nummer 1 bis 3 Voraussetzungen für die Errichtung gemeinsamer Dateien, welche jeweils die einzelfallbezogene Auslegung unbestimmter Rechtsbegriffe durch das Bundesamt für Verfassungsschutz erfordern. Dieses muss entscheiden, ob die Erforschung von Bestrebungen oder Tätigkeiten, die sich auf bestimmte Ereignisse oder Personenkreise beziehen, "von erheblichem Sicherheitsinteresse" für die Bundesrepublik Deutschland und den jeweils teilnehmenden Staat ist (§ 22b Absatz 1 Nummer 1 BVerfSchG-E). Es hat zu beurteilen, ob in den teilnehmenden Staaten "die Einhaltung grundlegender rechtsstaatlicher Prinzipien" gewährleistet ist (§ 22b Absatz 1 Nummer 2 BVerfSchG-E) und ob die Festlegungen und Zusagen dieser Staaten nach § 22b Absatz 5 BVerfSchG-E "verlässlich" sind.

Das Bundesverfassungsgericht hat zur Entscheidung über die Übermittlung personenbezogener Daten im Hinblick auf die Einschätzung, ob die Empfängerstaaten ein hinreichendes Schutzniveau bieten, ausgeführt:

"Die Vergewisserung über das geforderte Schutzniveau - sei es generalisiert, sei es im Einzelfall - ist eine nicht der freien politischen Disposition unterliegende Entscheidung deutscher Stellen. Sie hat sich auf gehaltvolle wie realitätsbezogene Informationen zu stützen und muss regelmäßig aktualisiert werden. Ihre Gründe müssen nachvollziehbar dokumentiert werden. Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können." (vgl. BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09, Rn. 339 mit weiteren Nachweisen).

Diese Vorgaben müssen auch für die Errichtung einer gemeinsamen Datei gelten, mittels derer teilnehmende Staaten Zugriff auf personenbezogene Daten erlangen. Um zu gewährleisten, dass die Entscheidung des Bundesamtes für Verfassungsschutz einer wirksamen gerichtlichen Kontrolle zugeführt werden kann, ist sicherzustellen, dass die Entscheidungsgrundlage schriftlich dokumentiert wird. Um der Vorgabe des Bundesverfassungsgerichts zu genügen, wird mit der Änderung eine Dokumentationspflicht für das Vorliegen der Voraussetzungen gemäß § 22b Absatz 1 Satz 1 BVerfSchG-E vorgesehen.

4. Zu Artikel 1 Nummer 2 (§ 22b Absatz 2 Satz 2 und 3 BVerfSchG)

In Artikel 1 Nummer 2 ist § 22b Absatz 2 wie folgt zu ändern:

a) Satz 2 ist wie folgt zu fassen:

"Dies ist der Fall, wenn Bestrebungen oder Tätigkeiten erforscht werden, von denen schwerwiegende Gefahren für die in § 3 Absatz 1 genannten Schutzgüter ausgehen."

b) Satz 3 ist zu streichen.

Begründung:

Der in § 22b Absatz 2 Satz 2 und 3 BVerfSchG-E zur Konkretisierung des Erfordernisses "besonderer Sicherheitsinteressen" verwendete Begriff der "schwerwiegenden Straftaten" ist in mehrfacher Hinsicht problematisch. Zum einen wird neben dem in § 100a Absatz 2 StPO legaldefinierten Begriff der "schweren Straftat" ein fast gleichlautender Begriff mit anderem Inhalt eingeführt, was zwar im Hinblick auf die Relativität juristischer Begriffe möglich, aber zumindest für die praktische Handhabung nicht besonders glücklich ist. Zum anderen hat das Bundesverfassungsgericht im Urteil zur Vorratsdatenspeicherung die Regelungstechnik, den Datenzugriff unter Bezugnahme auf Straftatenkataloge zu normieren, für ungeeignet befunden - wörtlich: "Den Datenzugriff unter Bezugnahme auf Kataloge von bestimmten Straftaten zu eröffnen, deren Verhinderung die Datenverwendung dienen soll [...], ist hier keine geeignete Regelungstechnik" (BVerfGE 125, 260 = NJW 2010, 833, 841; Rn. 230).

Generell erscheint fraglich, ob es regelungstechnisch sinnvoll ist, einen unbestimmten Rechtsbegriff durch einen anderen unbestimmten Rechtsbegriff zu definieren. Statt der Begriffsdefinitionen in § 22b Absatz 2 Satz 1 bis 3 BVerfSchG-E würde sich eher eine an bereits vorhandenen Begrifflichkeiten orientierende Terminologie empfehlen, zum Beispiel der in § 8a BVerfSchG verwendete Ausdruck "schwerwiegende Gefahren für die in § 3 Absatz 1 genannten Schutzgüter".

5. Zu Artikel 1 Nummer 2 (§ 22b Absatz 3 BVerfSchG)

In Artikel 1 Nummer 2 ist § 22b Absatz 3 wie folgt zu fassen:

"(3) Für die zu speichernden Datenarten und die Art der Speicherung gelten die §§ 3 und 4 Absatz 3 des Antiterrordateigesetzes entsprechend."

Begründung:

Die Formulierung von § 22b Absatz 3 Satz 1 BVerfSchG-E als Zweckbestimmung irritiert, da der Zweck der gemeinsamen Dateien schon in § 22b Absatz 1 BVerfSchG-E festgelegt wird.

Tatsächlich geht es um die Funktionsweise der Dateien, die ähnlich wie in den Fällen der verdeckten Speicherung nach § 4 ATDG zur Kontaktabklärung zwischen der abfragenden Behörde und der sich im Besitz der abgefragten Information befindlichen Behörde dienen sollen. Da die Funktionsweise erst in den bisherigen Sätzen 2 und 3 beschrieben wird, kommt dem Satz 1 kein eigenständiger Regelungsgehalt zu.

Die Bestimmung in § 22b Absatz 3 Satz 2 BVerfSchG-E über die zu speichernden Datenarten ist zu unbestimmt und weit. Zur Identifizierung von Personen können letztlich alle personenbezogenen Daten notwendig werden. Im Ergebnis erlaubt die Vorschrift damit die umfassende Speicherung aller verfügbaren personenbezogenen Daten, ohne dass diese wie in § 3 ATDG genauer festgelegt werden. Auch fehlt eine Regelung zum Umgang mit kennzeichnungspflichtigen Daten (vgl. § 3 Absatz 3 ATDG) und zum Schutz von personenbezogenen Daten, die mit besonders eingriffsintensiven Maßnahmen gewonnen wurden (vgl. § 4 Absatz 3 ATDG).

6. Zu Artikel 1 Nummer 2 (§ 22b Absatz 6 BVerfSchG)

In Artikel 1 Nummer 2 ist § 22b Absatz 6 wie folgt zu fassen:

"(6) § 6 Absatz 2 Satz 4 und 5, § 10 Absatz 1 und 2, §§ 11, 12 Absatz 1 bis 3 sowie § 19 gelten entsprechend mit der Maßgabe, dass die Eingabe durch das Bundesamt für Verfassungsschutz nur zulässig ist, wenn die Daten allen teilnehmenden ausländischen Nachrichtendiensten übermittelt werden dürfen."

Begründung:

Die Formulierung des § 22b Absatz 6 BVerfSchG-E erschwert durch die Benennung des Inhalts der Vorschriften, deren entsprechende Anwendung angeordnet wird, die Lesbarkeit. Auch irritiert die von § 22a Absatz 2 Satz 1 BVerfSchG abweichende Formulierung für das Erfordernis, dass die Datenübermittlung zulässig sein muss (dort entsprechende Anwendung).

7. Zu Artikel 1 Nummer 2 (§ 22b Absatz 7 Satz 2 BVerfSchG)

In Artikel 1 Nummer 2 sind in § 22b Absatz 7 Satz 2 die Wörter "nur für die vom Bundesamt für Verfassungsschutz eingegebenen Daten sowie dessen Abrufe." durch die Wörter "entsprechend mit der Maßgabe, dass sie nur für die vom Bundesamt für Verfassungsschutz eingegebenen Daten sowie dessen Abrufe zur Anwendung kommen." zu ersetzen.

Begründung:

In § 22b Absatz 7 Satz 2 BVerfSchG-E wird der Anwendungsbereich von § 6 Absatz 3 Satz 2 bis 5 BVerfSchG auf die vom Bundesamt für Verfassungsschutz eingegebenen Daten beschränkt. § 6 Absatz 3 BVerfSchG gilt aber nur für die gemeinsamen Dateien der Verfassungsschutzbehörden nach § 6 Absatz 2 BVerfSchG. Daher ist die entsprechende Anwendung der Vorschrift mit einschränkender Maßgabe anzuordnen.

8. Zu Artikel 1 Nummer 2 (§ 22b Absatz 8 - neu -, § 22c Satz 2 BVerfSchG)

Artikel 1 Nummer 2 ist wie folgt zu ändern:

a) Dem § 22b ist folgender Absatz anzufügen:

"(8) Das Bundesamt für Verfassungsschutz stellt sicher, dass die Landesbehörden für Verfassungsschutz vollen lesenden Zugriff auf die in den nach dieser Vorschrift errichteten gemeinsamen Dateien enthaltenen Daten erhalten. Die beteiligten ausländischen Nachrichtendienste sind hierauf bei Errichtung der gemeinsamen Datei hinzuweisen."

b) In § 22c Satz 2 ist die Angabe "und 6" durch die Angabe ",6 und 8" zu ersetzen.

Begründung:

Die Zusammenarbeit mit ausländischen Nachrichtendiensten in gemeinsamen Dateien als Kernstück des Gesetzentwurfs sieht keine Partizipation der Landesbehörden für Verfassungsschutz vor. Auch in der Gesetzesbegründung wird hierauf nicht eingegangen. Der in Artikel 73 Absatz 1 Nummer 10 Buchstabe b und c GG verankerte Verbundgedanke im Bereich des Verfassungsschutzes ist damit nicht einmal ansatzweise erkennbar. Das Bundesamt für Verfassungsschutz kann wegen der verfassungsrechtlichen Ausgestaltung des Verfassungsschutzverbundes als Mischverwaltung von Bund und Ländern nicht alleiniger Kommunikationspartner ausländischer Nachrichtendienste sein. Empfänger in der Bundesrepublik Deutschland ist "der deutsche Inlandsnachrichtendienst",

das heißt der Verfassungsschutzverbund insgesamt, nicht das Bundesamt für Verfassungsschutz isoliert.

Im Übrigen muss sichergestellt sein, dass erforderliche Daten aus der Datei vom Bundesamt für Verfassungsschutz nicht mit Weitergabesperren versehen werden dürfen, sondern zur Sicherung der Weitergabefähigkeit die Partner in einem Staatsvertrag aktiv auf das Verbundsystem in Deutschland hingewiesen werden müssen. Die Landesbehörden für Verfassungsschutz sind nicht "Dritte" im Sinne des Gesetzes.

9. Zu Artikel 3 Nummer 1 Buchstabe c (§ 28 Absatz 9 Satz 4 BPolG)

In Artikel 3 Nummer 1 Buchstabe c ist in § 28 Absatz 9 Satz 4 der Punkt am Ende durch die Wörter ", eine weitere Verwendung der Daten gegen die in Absatz 7 Satz 1 genannten Personen ausgeschlossen ist und die Daten gelöscht werden." zu ersetzen.

Begründung:

§ 28 Absatz 9 Satz 4 BPolG-E entspricht § 20w Absatz 3 Satz 5 BKAG. Diese Vorschrift hat das BVerfG jüngst für verfassungsgemäß erklärt (vgl. BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, juris, Rn. 262). Allerdings hat das BVerfG die Vorschrift verfassungskonform dahingehend ausgelegt, dass die Entscheidung über ein endgültiges Absehen von der Benachrichtigung voraussetzt, dass eine weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht werden. Diese weiteren Voraussetzungen sollten ausdrücklich in das Gesetz aufgenommen werden.

10. Zu Artikel 9 Nummer 2 (§ 111 Absatz 1 Satz 3 TKG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob in Artikel 9 Nummer 2 § 111 Absatz 1 Satz 3 TKG-E die Wörter "im Voraus bezahlten" gestrichen werden sollten, um nicht nur bei im Voraus bezahlten, sondern bei allen Mobilfunkdiensten eine Pflicht zur Prüfung der Richtigkeit der nach § 111 Absatz 1 Satz 1 TKG-E erhobenen Daten vor der Freischaltung vorzusehen.

Begründung:

§ 111 Absatz 1 Satz 1 und 3 TKG verpflichtet geschäftsmäßige Anbieter von Telekommunikations(TK)-Diensten bereits in der heute geltenden Fassung dazu, vor der Freischaltung bestimmte Teilnehmerdaten in Erfahrung zu bringen und zu speichern. Zu den Teilnehmerdaten gehören zum einen die Anschlusskennungen und gegebenenfalls die Mobilfunkendgerätenummern sowie zum anderen die wichtigsten persönlichen Daten des Vertragspartners wie Name,

Anschrift und Geburtsdatum. Sinn der Datenerhebung und -speicherung ist es, eine Datenbasis für die in den §§ 112 und 113 TKG geregelten Auskunftsverfahren zu schaffen. Die auskunftsberechtigten Sicherheitsbehörden (Strafvollzugsbehörden, Polizeivollzugsbehörden, Verfassungsschutzbehörden und so weiter) sollen im Rahmen ihrer Aufgabenerfüllung die Möglichkeit erhalten, Anschlusskennungen bestimmten Anschlussinhabern zuzuordnen.

Bislang gab es aber auch bei Prepaid-Produkten keine ausdrückliche Verpflichtung zur Überprüfung der erhobenen Daten. Die Begründung des Gesetzentwurfs hebt daher auf Seite 33 der BR-Drucksache 295/16 zutreffend die Bedeutung der Verifizierungspflicht bei der Erhebung der Kundendaten hervor. Ohne Ausweiskontrollpflicht können keine verlässlichen Daten erhoben werden und ohne eine solide Datenbasis können die Sicherheitsbehörden ihre Aufgaben nicht erfüllen. Sinn und Zweck des § 111 TKG-E, nämlich die Wahrung der Interessen der öffentlichen Sicherheit, die zu den anerkannten Zielen der TK-Regulierung (§ 2 Absatz 2 Nummer 9 TKG) gehört, sind nur so zu erreichen.

Es erscheint allerdings inkonsequent, die Verifizierungspflicht nur für Prepaid-Produkte einzuführen. Der Gesetzentwurf definiert nicht, was unter "im Voraus bezahlt" im Einzelnen zu verstehen ist. Da die Verifizierungspflicht zusätzlichen Aufwand und damit zusätzliche Kosten auf Seiten der TK-Unternehmen und deren Beauftragten verursacht wird, besteht die Gefahr, dass Umgehungsmodelle mit alternativen Bezahlmethoden, die aber nicht im Voraus erfolgen, eingeführt werden (zum Beispiel Bitcoin). Wenn man die Überprüfungspflicht für Kundendaten allein dadurch umgehen kann, dass die Dienste im Nachhinein bezahlt werden, wird diese Lücke wahrscheinlich ausgenutzt werden. Das Risiko des Forderungsausfalls kann auf andere Weise als durch Vorlage eines Ausweises umgangen werden, etwa durch Sicherheitsleistung (die rechtlich keine "Bezahlung" darstellt) in Form eines anonym hinterlegten Betrages in Bitcoin oder einer anderen anonymen digitalen Währungseinheit.

Gerade weil die meisten Anbieter von nicht im Voraus bezahlten Mobilfunkdiensten schon heute auf Grundlage von § 95 TKG einen Ausweis verlangen (obwohl sie es nicht müssen), kann man durch die Streichung der Wörter "im Voraus bezahlte" ohne großen Aufwand sicherstellen, dass zukünftig bei allen Mobilfunkverträgen lückenlos eine Identitätsprüfung erfolgt.