Ausarbeitung

Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikationsüberwachung durch Nachrichtendienste

Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts der Bundesregierung

Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikationsüberwachung durch Nachrichtendienste
Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts der Bundesregierung

Aktenzeichen: WD 3 - 3000 - 293/20
Abschluss der Arbeit: 19. Februar 2021
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Einleitung und Fragestellung

Die Bundesregierung hat Ende November 2020 den Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts in den Bundestag eingebracht.[1] Dieser sieht insbesondere vor, die Regelungen zur Telekommunikationsüberwachung (TKÜ) des § 11 Artikel 10-Gesetz (G 10)[2] um eine Regelung der Durchführung als **Quellen-TKÜ** zu ergänzen, „um die Aufklärung schwerer Bedrohungen für unseren demokratischen Rechtsstaat und die freiheitlich demokratische Grundordnung zu gewährleisten“[3]. Damit würden **alle Nachrichtendienste** die Befugnis zum Einsatz der Quellen-TKÜ erhalten.

Die Quellen-TKÜ ist eine besondere Form der TKÜ, die der Überwachung von Kommunikation über Kommunikationsprogramme dient, die standardmäßig eine **Verschlüsselung** ihrer Kommunikationsdaten und -inhalte nutzen. Die Quellen-TKÜ erfasst die Kommunikation „an der Quelle“, bevor diese verschlüsselt wird oder nachdem diese entschlüsselt wurde.[4] Dazu bedarf es einer speziellen **Überwachungssoftware,** die die verdeckte Überwachung möglich macht. Diese wird umgangssprachlich als **Staatstrojaner** bezeichnet.

Auf Bundesebene ist die Quellen-TKÜ als strafprozessuale Maßnahme gesetzlich in § 100a Abs. 1 S. 2 und S. 3 Strafprozessordnung (StPO)[5] geregelt; gemäß § 5, § 51 Abs. 2 Bundeskriminalamtgesetz (BKAG)[6] kann das Bundeskriminalamt die Quellen-TKÜ zur Abwehr von Gefahren des internationalen Terrorismus einsetzen. Einige Landesverfassungsschutzgesetze sehen für die jeweiligen Landesämter für Verfassungsschutz die Befugnis zur Quellen-TKÜ vor (vgl. bspw. § 13 Bayerisches Verfassungsschutzgesetz[7] sowie § 8 Abs. 12 Hamburgisches Verfassungsschutzgesetz[8]). Presseberichten zufolge wurden mehrere Verfassungsbeschwerden gegen die Regelungen

---

1 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, vom 27. November 2020, BT-Drs. 19/24785.

2 Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2007 I S. 154), das zuletzt durch Artikel 38 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

3 Gesetzentwurf, BT-Drs. 19/24785, 1.

4 Information des BKA zur Quellen-TKÜ, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html (letzter Abruf 17. Februar 2021).

5 Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 49 des Gesetzes vom 21. Dezember 2020 (BGBl. I S. 3096) geändert worden ist.

6 Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das durch Artikel 5 des Gesetzes vom 3. Dezember 2020 (BGBl. I S. 2744) geändert worden ist.

7 Bayerisches Verfassungsschutzgesetz (BayVSG) vom 12. Juli 2016 (GVBl. S. 145, BayRS 12-1-I), das zuletzt durch § 1 Abs. 14 der Verordnung vom 26. März 2019 (GVBl. S. 98) geändert worden ist.

8 Hamburgisches Verfassungsschutzgesetz (HmbVerfSchG) vom 7. März 1995, zuletzt geändert durch Artikel 1 des Gesetzes vom 24. Januar 2020 (HmbGVBl. S. 99).

der Quellen-TKÜ in der StPO sowie im Hamburgischen Verfassungsschutzgesetz beim Bundesverfassungsgericht eingereicht.[9]

Gefragt wird, wie die Regelung zur Quellen-TKÜ im Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzgesetzes verfassungsrechtlich zu bewerten ist, sowie ob es klare Voraussetzungen gibt, denen der Einsatz von Staatstrojanern durch Nachrichtendienste unterliegen muss. Weiter wird gefragt, ob sich die Regelung mit dem verfassungsrechtlichen Trennungsprinzip zwischen Strafverfolgungs- und Polizeibehörden auf der einen sowie den Nachrichtendiensten auf der anderen Seite vereinbaren lässt.

2. Regelungen zur Quellen-TKÜ im Gesetzentwurf

Der Gesetzentwurf der Bundesregierung sieht vor, § 11 G 10 um zwei neue Absätze 1a und 1b zu ergänzen. Die **Befugnis zur Quellen-TKÜ** regelt der **neue Absatz 1a,** der der Befugnis in § 100a Abs. 1 S. 2, S. 3, Abs. 5, Abs. 6 StPO nachgebildet ist. Dieser soll auszugsweise wie folgt lauten:

> „(1a) Die Überwachung und Aufzeichnung der laufenden Telekommunikation, die nach dem Zeitpunkt der Anordnung übertragen worden ist, darf auch in der Art und Weise erfolgen, dass in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen ab dem Zeitpunkt der Anordnung gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Bei den Maßnahmen nach den Sätzen 1 und 2 ist technisch sicherzustellen, dass
>
> 1. ausschließlich überwacht und aufgezeichnet werden können:
>
> a) die laufende Kommunikation (Satz 1) und
>
> b) Inhalte und Umstände der Kommunikation, die auch während des laufenden Kommunikationsvorgangs ab dem Zeitpunkt der Anordnung im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Satz 2),
>
> 2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,
>
> 3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

9 Digitalcourage: Verfassungsbeschwerde gegen Staatstrojaner eingereicht, ZD-Aktuell 2018, 06241; GFF: Verfassungsbeschwerde gegen baden-württembergisches Polizeigesetz, ZD-Aktuell 2019, 06405.

> Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. […]“

§ 11 Abs. 1b G 10-E regelt die Möglichkeit einer **technischen Erweiterung** der gegen eine Person laufenden Maßnahme über **weitere Kennungen** von Telekommunikationsanschlüssen dieser von der Maßnahme betroffenen Person.

3. Verletzung des Fernmeldegeheimnisses gemäß Art. 10 Abs. 1 GG

Die Kommunikationsteilnehmer könnten in ihrem Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG verletzt sein.

3.1. Schutzbereich

Das Fernmeldegeheimnis schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des **Telekommunikationsverkehrs**.[10] Dies umfasst sowohl den **Inhalt** der Telekommunikation als auch die **näheren Umstände** des Fernmeldevorgangs. Das Grundrecht ist **entwicklungsoffen** und umfasst auch neuartige Übertragungstechniken, einerlei welche Übermittlungsart und welche Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) genutzt werden.[11] **Außerhalb** des **laufenden Kommunikationsvorgangs** werden die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation jedoch nicht durch Art. 10 Abs. 1 GG geschützt. Persönlich sind die **Teilnehmer** des Kommunikationsvorgangs, d.h. Absender und Empfänger, Träger des Grundrechts.[12] Inhalte und Umstände von laufenden Kommunikationsvorgängen, durch die auf Grundlage von § 11 Abs. 1a G 10-E zugegriffen werden kann, würden demnach grundsätzlich Art. 10 Abs. 1 GG unterfallen.

Problematisch ist indes die **Abgrenzung zum IT-Grundrecht** gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Dieses soll vor heimlichen Zugriffen schützen, durch die die **auf dem System vorhandenen Daten** ganz oder zu wesentlichen Teilen ausgespäht werden können (Online-Durchsuchung).[13] Nach der Rechtsprechung des **Bundesverfassungsgerichts** muss sich die **Quellen-TKÜ alleine** an **Art. 10 Abs. 1 GG** messen lassen, **wenn** sich die Überwachung ausschließlich auf Daten aus einem **laufenden** Telekommunikationsvorgang beschränkt.[14] Die Quellen-TKÜ habe lediglich die Aufgabe, den technischen Entwicklungen der Informationstechnik zu folgen und – ohne Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems – eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich sei. Demnach wäre hier **§ 11 Abs. 1a S. 1 G 10-E,** welcher ausdrücklich (nur)

---

10 Zum Folgenden BVerfGE 115, 166 (182 f.).

11 BVerfGE 120, 274 (307); Ogorek, in: Epping/Hillgruber (Hrsg.), BeckOK Grundgesetz, 45. Edition, Stand: 15.11.2020, Art. 10 Rn. 37.

12 BVerwG, Urteil vom 30. Mai 2018, Az. 6 A 3/16, NVwZ 2018, 1476 (1479), Rn. 27.

13 BVerfGE 120, 274 (314).

14 BVerfGE 120, 274 (309); BVerfGE 141, 220 (309, Rn. 228).

zum Zugriff auf die laufende Kommunikation ermächtigen soll, grundsätzlich nur am Maßstab des Art. 10 Abs. 1 GG zu messen.

Anders stellt sich dies für die Vorschrift des **§ 11 Abs. 1a S. 2 G 10-E** dar. Danach dürfen nicht nur Inhalte und Umstände der Kommunikation eines laufenden Kommunikationsvorgangs überwacht und aufgezeichnet, sondern **auch vergangene Kommunikationsdaten** erfasst werden – also solche, die zwischen dem Zeitpunkt der Anordnung und der Installation und Inbetriebnahme der Spähsoftware auf den Endgeräten gespeichert worden sind. Bei diesen Daten ist es äußerst zweifelhaft, ob noch von einem Funktionsäquivalent zur laufenden, unverschlüsselten Kommunikation ausgegangen werden kann, da kein unmittelbarer Bezug zum Übertragungsvorgang mehr gegeben ist. In der Literatur wird zu Recht darauf hingewiesen, dass auch bei einer klassischen TKÜ die tatsächliche Überwachung stets erst mit dem technischen Zugriff auf den Übertragungsweg beginnt und dieser Zeitpunkt stets erst nach Ergehen der Anordnung liegt.[15] Zwar beschränkt § 11 Abs. 1a S. 2 G 10-E den Eingriff auf solche Kommunikationsinhalte und -umstände, die „auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“. Diese Einschränkung ändert aber nichts daran, dass in zeitlicher Hinsicht die Zulässigkeit des Eingriffs eindeutig an den Zeitpunkt der Anordnung anknüpft. Dieser Befund wird noch durch flankierende Regelungen in den Sätzen 1 und 3 unterstützt. Über eine Befugnis zur Quellen-TKÜ, die mit dem **Zeitpunkt der Anordnung** und nicht erst zum Zeitpunkt des technischen Einsatzes einsetzt, hat das Bundesverfassungsgericht bisher noch nicht entschieden. Es spricht viel dafür, dass der Eingriff in Kommunikationsdaten, die zeitlich schon vor der technischen Infiltration angekommen sind, an den **strengeren Maßstäben der Online-Durchsuchung zu messen** ist[16] (siehe dazu unter **4.**).

3.2. Eingriff

In das Grundrecht wird nicht nur durch jede **Kenntnisnahme, Aufzeichnung und Verwertung** kommunikativer Daten eingegriffen, sondern bereits durch die **Anordnung** des Zugriffs.[17] Dementsprechend ermächtigt **§ 11 Abs. 1a S. 1 G 10-E**, wonach auf die laufende Kommunikation durch Eingriff in ein informationstechnisches System zugegriffen werden kann, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen, zu **Eingriffen** in Art. 10 Abs. 1 GG.

3.3. Rechtfertigung

Der Eingriff ist gerechtfertigt, wenn das eingreifende Gesetz dem Zitiergebot gemäß Art. 19 Abs. 1 S. 2 GG entspricht, weiterhin insbesondere die Anforderungen des Bestimmtheitsgebots eingehalten sind und der Eingriff verhältnismäßig ist.

---

15 Freiling/Safferling/Rückert, Juristische Rundschau 2018, 9 (12); vgl. auch Roggan, StV 2017, 821 (824).

16 So auch Singelnstein/Derin, NJW 2017, 2646 (2648); Freiling/Safferling/Rückert, Juristische Rundschau 2018, 9 (21); Roggan, StV 2017, 821 (824); Martini/Fröhlingsdorf, NVwZ 2020, 1803 (1804), Fn. 10.

17 BVerfGE 124, 43 (58).

Dem **Zitiergebot** ist mit Art. 6 des vorliegend zu prüfenden Gesetzentwurfs Rechnung getragen, welcher feststellt, dass durch § 11 Abs. 1a G 10-E Art. 10 Abs. 1 GG eingeschränkt wird. Auch an der **Bestimmtheit**[18] der Eingriffsbefugnis in § 11 Abs. 1a G 10-E bestehen keine durchgreifenden Bedenken; im direkten Vergleich zu § 100a StPO scheint der Gesetzgeber eher noch Präzisierungen vorzunehmen.

3.3.1. Verhältnismäßigkeit

Der Grundsatz der Verhältnismäßigkeit setzt voraus, dass der Eingriff einen legitimen Zweck in geeigneter, erforderlicher und angemessener Weise verfolgt.

3.3.1.1. Legitimer Zweck

Nach der Rechtsprechung des Bundesverfassungsgerichts ist die **Effektivierung** der **Erfüllung** der **Aufgaben** der **Nachrichtendienste** ein **legitimer Gemeinwohlzweck.**[19] Nach der Begründung des hier zu prüfenden Gesetzentwurfs erfordern die „aktuellen Herausforderungen insbesondere im Bereich des internationalen Terrorismus und des Rechtsterrorismus […] eine Anpassung der Befugnisse, um die Aufklärung schwerer Bedrohungen für unseren demokratischen Rechtsstaat und die freiheitlich demokratische Grundordnung zu gewährleisten.“[20] Die Befugnis zur Quellen-TKÜ ist eine Reaktion auf „die gewandelten Kommunikationsgewohnheiten unter Nutzung moderner Technik“[21] und soll die bestehende „Aufklärungslücke bei Messengerdiensten, die technisch aus dem Speicherplatz des Endgeräts – unverschlüsselt – ausgelesen werden müssen“[22] schließen. Damit verfolgt der Gesetzgeber einen legitimen Zweck.

3.3.1.2. Geeignetheit

An der Geeignetheit der Quellen-TKÜ für die Effektivierung der Aufgabenerfüllung der Nachrichtendienste bestehen keine Zweifel. Diese **schließen** eine **Lücke** der Beobachtungsmöglichkeiten, die durch die technischen Verschlüsselungsmöglichkeiten gewandelter Kommunikationsformate entstanden sind.

3.3.1.3. Erforderlichkeit

Die Quellen-TKÜ müsste zudem erforderlich sein, d.h. es dürfte kein milderes aber gleich effektives Mittel bestehen.[23] Als milderes Mittel gegenüber dem Einsatz einer Ausspähsoftware wird z.T.

---

18 Siehe dazu Martini, in: v. Münch/Kunig (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 7. Auflage 2021, Art. 10 Rn. 130.

19 BVerfGE 125, 260 (316).

20 Gesetzentwurf, BT-Drs. 19/24785, 1.

21 Ebenda, 13.

22 Ebenda, 22.

23 Grzeszick, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, Werkstand: 92. EL August 2020, Art. 20 Rn. 113.

diskutiert, die **Anbieter** der **verschlüsselten Kommunikationstechniken** zu **verpflichten,** den Nachrichtendiensten auf Anordnung **unverschlüsselte Daten** bzw. einen **Schlüssel** für die verschlüsselten Daten zur Verfügung zu stellen.[24] Ein solcher „Generalschlüssel" birgt jedoch die Gefahr, dass allgemein das Vertrauen in die Vertraulichkeit neuer Kommunikationsformen insgesamt erschüttert werden könnte. Insofern wäre die Alternative jedenfalls nicht milder.

3.3.1.4. Angemessenheit

Die Einführung einer Befugnis zur Quellen-TKÜ müsste schließlich angemessen sein, d.h. sie darf nicht außer Verhältnis zum Zweck bzw. Ziel der Maßnahme stehen. Das Gebot der Angemessenheit erfordert „eine Abwägung zwischen dem Nutzen der Maßnahme und den durch die Maßnahmen herbeigeführten Beeinträchtigungen und setzt dem Ergebnis eine Grenze"[25].

Die Überwachung der laufenden Telekommunikation begründet nach der Rechtsprechung des Bundesverfassungsgerichts einen **schwer wiegenden Eingriff.**[26] Die Intensität des Eingriffs verschärft sich hier nicht nur durch die **Heimlichkeit** der Überwachung, sondern zudem dadurch, dass **Schutzmaßnahmen umgangen** werden, die der Betroffene zur Wahrung der Vertraulichkeit ergriffen hat. Hinzu tritt die **Streubreite** der betroffenen Personen. Es ist zu beachten, dass nach § 11 Abs. 1a G 10-E zwar **technisch** in ein **gesamtes informationstechnisches System** (bspw. das gesamte Endgerät) eingegriffen werden kann, dabei aber der Zugriff rechtlich **auf laufende Kommunikationsdaten** beschränkt ist. Auch wenn die Eingriffsbefugnis somit punktuell auf individuelle Kommunikationsvorgänge beschränkt ist, so ist doch von einer gewissen Streubreite auszugehen, da nicht nur Informationen über das Kommunikationsverhalten desjenigen gewonnen werden, gegen den sich die Maßnahme richtet, sondern auch über das seiner Kommunikationspartner. Zudem können gemäß § 3 Abs. 2 S. 2 G 10 auch die Anschlüsse von für den Eingriffsanlass **nicht verantwortliche Personen** überwacht werden, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass der Verdächtige ihren Anschluss nutzt. Die Eingriffsintensität kann sich auch durch die Schaffung von Sicherheitslücken durch Staat verschärfen (siehe hierzu unter 3.3.1.4.6.).

Dem stehen mit dem Schutz der verfassungsmäßigen Ordnung, dem Bestand und der Sicherheit von Bund und Ländern sowie von Leib, Leben und Freiheit der Person vor Bedrohungen des internationalen und nationalen Terrorismus **Schutzgüter** und **Verfassungswerte von hohem verfassungsrechtlichem Gewicht** gegenüber[27]. Nach Ansicht des Bundesverfassungsgerichts sind zur Terrorismusabwehr auch schwer wiegende Eingriffe gerechtfertigt, sofern die Eingriffsgrundlagen **im Einzelnen**

---

24 Buermeyer, Technische Grundlagen und rechtliche Grenzen der Quellen-Kommunikationsüberwachung, Beitrag zum 37. Strafverteidigertag, Freiburg 2013, abrufbar unter http://www.strafverteidiger-vereinigungen.de/Material/Themen/Technik%20&%20Ueberwachung/37_buermeyer.pdf (letzter Abruf 17. Februar 2020); siehe auch Martini/Fröhlingsdorf, NVwZ 2020, 1803 (1804).

25 Grzeszick, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, Werkstand: 92. EL August 2020, Art. 20 Rn. 117.

26 BVerfGE 141, 220 (310, Rn. 229).

27 BVerfGE 141, 220 (267, Rn. 100); BVerfGE 120, 274 (Ls. 2, 319).

verhältnismäßig begrenzt sind. Als Kriterien nennt es die Gestaltung der **Eingriffsschwellen,** die **Zahl** der **Betroffenen** und die **Intensität** der **Beeinträchtigungen.**[28]

3.3.1.4.1. Eingriffsschwelle

Der Einsatz der Quellen-TKÜ setzt voraus, dass **tatsächliche Anhaltspunkte** für den **Verdacht** bestehen, dass jemand eine der in Absatz 1 aufgelisteten **Katalogtaten** plant, begeht oder begangen hat (§ 3 Abs. 1 S. 1 G 10) oder dass tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand **Mitglied einer Vereinigung** ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die **freiheitliche demokratische Grundordnung,** den **Bestand** oder die **Sicherheit** des **Bundes** oder eines **Landes** gerichtet sind (§ 3 Abs. 1 S. 2 G 10). Die Eingriffsschwelle der tatsächlichen Anhaltspunkte des § 3 Abs. 1 G 10 ist im Vergleich zu den Anforderungen der „bestimmten Tatsachen", die die Quellen-TKÜ zur Strafverfolgung rechtfertigen (§ 100a Abs. 1 StPO), niedriger.

Schon an der bestehenden Befugnis zur klassischen TKÜ wird sowohl mit Blick auf die tatbestandliche Schwelle des § 3 Abs. 1 G 10 als auch auf einige der Straftaten aus dem Katalog des § 3 Abs. 1 G 10 Kritik geübt.[29] Insbesondere wird bemängelt, dass es zum Teil an der von der Verhältnismäßigkeit geforderten **Begrenzung** auf **schwere Straftaten fehle**.[30] Aufgrund der gesteigerten Eingriffsintensität der Quellen-TKÜ kommt dieser Kritik noch größere Bedeutung zu. Das **Bundesverfassungsgericht** hat die **niedrige Schwelle** der tatsächlichen Anhaltspunkte in verfassungsrechtlicher Hinsicht allerdings bisher **nicht beanstandet**.[31]

Ein **ultima-ratio-Prinzip** in der Form, dass die Quellen-TKÜ nur als letztes Mittel zur Informationsgewinnung eingesetzt werden darf, ist aus der Rechtsprechung nicht herleitbar. Mit Blick auf die TKÜ ist allerdings davon auszugehen, dass eine Quellen-TKÜ erst dann erforderlich ist, wenn aufgrund der Verschlüsselung klassische TKÜ-Maßnahmen keinen Erfolg hätten, siehe insoweit auch den sog. Subsidiaritätsgrundsatz des § 11 Abs. 1a S. 1 G 10-E.

3.3.1.4.2. Technische Vorkehrungen

§ 11 Abs. 1a G 10-E sieht gegenüber den allgemeinen Anforderungen des § 4 G 10 (Prüf-, Kennzeichnungs- und Löschungspflichten, Übermittlungen und Zweckbindung) weitere zusätzliche Sicherungen vor: So ist gemäß § 11 Abs. 1a S. 3 Nr. 2 G 10-E sicherzustellen, dass **nur unerlässliche Veränderungen** der informationstechnischen Systeme vorgenommen werden, die – soweit technisch möglich – bei Beendigung der Maßnahme **automatisch rückgängig** gemacht werden. Gemäß § 11 Abs. 1a S. 4 G 10-E ist das eingesetzte Mittel nach dem Stand der Technik gegen **unbefugte**

28 BVerfGE 100, 313 (376).

29 Roggan, G-10-Gesetz, 2. Online-Auflage 2018, § 3 Rn. 7, 9 ff. mit Verweis auf BVerfGE 113, 348 (378); dagegen aber Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 3 G 10 Rn. 4 f. mit Verweis unter anderem auf BVerfGE 100, 313 (395).

30 Roggan, G-10-Gesetz, 2. Online-Auflage 2018, § 3 Rn. 9 ff.

31 Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 3 G 10 Rn. 5.

Nutzung zu **schützen;** zudem sind kopierte Daten nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Der Gesetzentwurf folgt damit den Anforderungen, die das Bundesverfassungsgericht für die Online-Durchsuchung aufgestellt hat.[32]

In der Literatur wird vielfach bezweifelt, ob es mit den derzeitigen technischen Mitteln überhaupt möglich ist, dass sich die Überwachung allein auf die laufende Kommunikation beziehe.[33] Das **Bundesverfassungsgericht** sah dies jedoch nur als rein tatsächliche Frage an, **nicht** als **verfassungsrechtliches Problem**.[34]

In der Literatur werden z.T. **detaillierte technische, organisatorische Vorkehrungen auf gesetzlicher Ebene** gefordert.[35] Es werden insbesondere gesetzliche Regelungen dazu, wer die Software programmiert und wer auf welche Weise ihre Eignung kontrolliert, aus Gründen des Wesentlichkeitsgebots für erforderlich gehalten.[36] Das Bundesverfassungsgericht äußerte allerdings keine solchen Bedenken gegenüber der Ermächtigung zur Quellen-TKÜ in § 50l BKAG a.F.[37]

3.3.1.4.3. Betroffenheit Dritter

Gemäß § 3 Abs. 2 S. 2 G 10 kann sich die Maßnahme neben der verdächtigen Zielperson auch gegen Unverdächtige richten, sogenannte **Nachrichtenmittler**. Die Einbeziehung von Nebenbetroffenen hat das Bundesverfassungsgericht in seinem ersten G 10-Urteil aus dem Jahr 1970 für **verfassungsrechtlich zulässig** gehalten;[38] das Gericht **fordert** aber eine **Eingrenzung.**[39] Diese Eingrenzung dürfte durch die tatbestandlichen Vorgaben des § 3 Abs. 2 S. 2 G 10 gewährleistet sein, wonach es **bestimmter Tatsachen** für die Annahme bedarf, dass die Person für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt. Ergänzt wird die Eingrenzung zudem durch die im Gesetzentwurf vorgesehene Ausnahmeregelung des **§ 11 Abs. 1b S. 2 G 10-E.** § 11 Abs. 1b S. 1 G 10-E sieht vor, dass eine Anordnung auf weitere Kennungen von Telekommunikationsanschlüssen der Person, gegen die sich die Anordnung richtet, erstreckt werden darf, wenn diese nach der Anordnung bekannt werden. **Ausgenommen** sind hiervon gemäß § 11 Abs. 1b S. 2 G 10-E jedoch Kennungen von

---

32 Vgl. BVerfGE 141, 220 (305, Rn. 215).

33 Siehe bspw. Martini, NwVZ 2020, 1893; Kipker, ZRP 2016, 88 (89); Braun, Kommunikation & Recht 2011, 681 (685).

34 BVerfGE 141, 220 (311, Rn. 234); anders zuvor noch LVerfG Sachsen-Anhalt, Urteil vom 11. November 2014, Az. LVG 9/13 (Rn. 196 ff.), LKV 2015, 33 (37); dem zustimmend Roggan, LKV 2015, 14 (17); Tomerius, NVwZ 2015, 412 (414 f.).

35 Martini, in: v. Münch/Kunig (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 7. Auflage 2021, Art. 10 Rn. 197.

36 Roggan, StV 2017, 821 (825).

37 Vgl. BVerfGE 141, 220 (309 ff., Rn. 227 ff.); siehe jetzt § 49 BKAG.

38 BVerfGE 30, 1 (22).

39 Vgl. BVerfGE 113, 348 (380 f.).

Telekommunikationsanschlüssen von Personen, gegen die sich die Anordnung richtet, weil auf Grund bestimmter Tatsachen anzunehmen ist, dass der Verdächtige ihren Anschluss benutzt.

3.3.1.4.4. Kernbereich privater Lebensgestaltung

Das Bundesverfassungsgericht fordert besondere gesetzliche Schutzvorkehrungen, die der Gesetzgeber mit Blick auf **höchstprivate Kommunikation,** die dem Schutz des **Kernbereichs privater Lebensgestaltung** unterliegt, zu treffen hat.

Auf der **Stufe der Datenerhebung** hat der Gesetzgeber dafür Sorge zu tragen, dass „die Erhebung kernbereichsbezogener Daten soweit wie informationstechnisch und ermittlungstechnisch **möglich unterbleibt**“[40]. Das Bundesverfassungsgericht fordert zudem, dass der Gesetzgeber durch **geeignete Verfahrensvorschriften** sicherstellt, dass dann, wenn kernbereichsbezogene Daten erhoben worden sind, „die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben“[41]. So ist eine **unverzügliche Löschung** dieser Daten sowie der **Ausschluss** einer **Weitergabe** oder **Verwertung** gefordert.[42] Nach Ansicht des Bundesverfassungsgerichts ist es nicht in jedem Fall zwingend, dass eine **unabhängige Stelle** mit der Sichtung automatisiert erhobener Daten zu betrauen ist.[43]

§ 3a G 10-E dürfte diesen **Anforderungen genügen.** Die geforderte Prüfung auf der Stufe der Datenerhebung regelt § 3a Abs. 1 S. 1 G 10-E: Danach ist eine Maßnahme unzulässig, wenn **tatsächliche Anhaltspunkte** für die Annahme vorliegen, dass durch sie allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst würden. Das Bundesverfassungsgericht hat bei einer ähnlich lautenden Regelung zwar das Wort „allein“ problematisiert, lässt diese Formulierung gleichwohl genügen, da sich diese verfassungskonform in der Form auslegen lasse, dass Gespräche nicht schon dann aus dem strikten Schutz herausfallen, wenn sich in ihnen Höchstpersönliches und Alltägliches vermischt.[44] Eine weitere Verfahrenssicherung regelt das Gebot des § 3a Abs. 1 S. 2 G 10-E, wonach die Maßnahme **unverzüglich zu unterbrechen** ist, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Weiter sieht § 3a Abs. 1 S. 4 G 10-E eine unverzügliche Sichtung von automatischen Aufzeichnungen durch eine **unabhängige Stelle,** ein Mitglied der G 10-Kommission, vor. § 3a Abs. 1 S. 8 G 10-E regelt ein **Verwertungsverbot** und ordnet die **unverzügliche Löschung** an. Die Tatsache der Datenerfassung und der Löschung ist zu dokumentieren, wobei diese **Dokumentation** ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden darf, § 3a Abs. 1 S. 9 und S. 10 G 10-E. Die **Aufbewahrungsfrist** der Dokumentation beträgt

40 BVerfGE 120, 274 (338) m.w.N., Hervorhebung nur hier.

41 BVerfGE 120, 274 (338).

42 BVerfGE 120, 274 (337).

43 BVerfGE 141, 220 (313 f., Rn. 240 f.).

44 BVerfGE 141, 220 (314 f., Rn. 243) m.w.N.

nach § 3a Abs. 1 S. 12 G 10-E **sechs Monate** und ist damit deutlich länger als die Aufbewahrungsfrist von drei Monaten, die vom Bundesverfassungsgericht im Jahr 2016 als verfassungswidrig angesehen wurde.[45]

Besondere Anforderungen sind an den **Schutz von Vertraulichkeitsbeziehungen** – wie insbesondere zwischen **Journalisten und ihren Informanten** oder **Rechtsanwälten und ihren Mandanten** – zu stellen. Grundrechtlicher Schutz folgt hier nicht nur z.B. aus der Pressefreiheit gemäß Art. 5 Abs. 1 S. 2 GG, sondern schon aus Art. 10 Abs. 1 GG und den sich hieraus ableitenden Verhältnismäßigkeitsanforderungen.[46] Der Schutz von Vertraulichkeitsbeziehungen – etwa bezüglich von Pressevertretern sowie Rechtsanwälten als **Berufsgeheimnisträger** wird durch **§ 3b G 10-E**, welcher auf § 53 StPO verweist, grundsätzlich gewährleistet.[47] Es ist zudem stets eine Abwägung im Einzelfall anzustellen.

3.3.1.4.5. Verfahrensrechtliche Vorkehrungen, insbesondere präventiver Richtervorbehalt und Rechtsschutz nach erfolgter Anordnung

Nach herrschender Meinung wird für die Anordnung heimlicher bzw. verdeckter Maßnahmen zur TKÜ ein präventiver **Richtervorbehalt** für notwendig erachtet.[48] Für Geheimdienste lässt das Bundesverfassungsgericht grundsätzlich auch eine **gerichtsähnliche Kontrolle** ausreichen.[49] Anstelle eines Richtervorbehalts sieht § 15 Abs. 6 S. 1 G 10-E dementsprechend eine **präventive Kontrolle durch** die **G 10-Kommission** vor, die als gerichtsähnliches Kontrollorgan eigener Art fungiert.[50] Die bereits bestehenden Vorkehrungen sollen durch verschiedene Regelungen im Gesetzentwurf noch weiter ausgebaut werden, indem die G 10-Kommission durch die **Erhöhung ihrer Mitgliederzahl** und erhöhte Anforderungen an ihre **volljuristische Qualifikation gestärkt** werden soll (vgl. § 15 G 10-E). Zudem wird das **Zustimmungserfordernis** der G 10-Kommission klarer formuliert und deren Kontrollrechte durch die **neue, detailliertere Regelung zur Eilanordnung** (§ 15a G 10-E) wohl gestärkt. Der Gesetzgeber trägt damit der gesteigerten Eingriffsintensität der Quellen-TKÜ Rechnung.

---

45 Vgl. BVerfGE 141, 220 (315 f., Rn. 246).

46 Vgl. BVerfG NJW 2020, 2235 (2253 f., Rn. 193 ff.).

47 Im Einzelnen kritisch Huber, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, § 3b G 10 Rn. 5.

48 Gusy, in: von Mangoldt/Klein/Starck (Hrsg.), Grundgesetz, 7. Auflage 2018, Art. 10 Rn. 77; Durner, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, Werkstand: 92. EL August 2020, Art. 10 Rn. 197 ff. m.w.N.

49 BVerfGE 30, 1 (28); BVerfG NJW 2020, 2235 (2252, Rn. 181) m.w.N.

50 Vgl. dazu auch Roggan, G-10-Gesetz, 2. Online-Auflage 2018, § 15 Rn. 1 f.

Den verfahrensrechtlichen Anforderungen an den **Rechtsschutz** nach erfolgter Anordnung kommt der Gesetzgeber zunächst über spezielle **Protokollierungspflichten** in § 11 Abs. 1a S. 5 G 10-E nach, die die geforderte wirksame Kontrolle überhaupt erst ermöglichen.[51]

Der Gesetzgeber hat bei heimlichen Eingriffen die Pflicht einer zumindest nachträglichen **Benachrichtigung** vorzusehen; dies ist ein **Gebot effektiven Grundrechtsschutzes**.[52] Allerdings kann nach der sog. Staatsschutzklausel gemäß **Art. 10 Abs. 2 S. 2 GG** von der Benachrichtigung zunächst **abgesehen** werden, wenn die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes dient. Die **eingeschränkten Benachrichtigungspflichten nach § 12 G 10**, welche auch auf die Anordnung der Quellen-TKÜ nach § 3 G 10 i.V.m. § 11 Abs. 1a G 10-E anwendbar sind, nutzen diesen Spielraum aus[53] und sind grundsätzlich nicht zu beanstanden.

Vor der Mitteilung ist nach **§ 13 G 10** der **Rechtsweg** gegen Anordnung und Vollzug von Beschränkungsmaßnahmen – wie der Anordnung einer Quellen-TKÜ – formell **ausgeschlossen**. Auch dies ist in Ausnutzung des Spielraums von Art. 10 Abs. 2 S. 2 GG mit dem Grundgesetz vereinbar, wenn durch ein **gerichtsähnliches Kontrollorgan** ein Nachprüfungsverfahren gewährleistet ist, welches dem Gerichtsschutz materiell und prozedural äquivalent ist.[54] Als gerichtsähnliches Kontrollorgan eigener Art fungiert insoweit die sachlich unabhängige und weisungsfreie **G 10-Kommission** gemäß **§ 15 G 10-E**[55]; § 15 Abs. 5 G 10-E sieht ein **Beschwerdeverfahren** vor der G 10-Kommission vor. Sobald dem Betroffenen die Maßnahme mitgeteilt wurde oder er von der Maßnahme auf anderem Wege erfahren hat[56], steht ihm der Verwaltungsrechtsweg offen.

3.3.1.4.6. Schaffung von Sicherheitslücken durch Staat

In der Literatur wird z.T. eingewandt, dass der Einsatz der technischen Mittel der Quellen-TKÜ unverhältnismäßig sei, da dies zu einer **massiven Gefährdung der Integrität und Vertraulichkeit informationstechnischer Systeme** und **nicht hinnehmbaren Risiken für die allgemeine IT-Sicherheit** führe.[57] Der Staat käme seinem Auftrag aus dem „verfassungsrechtliches Normensemble“ des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10, Art. 87f und Art. 91c GG, die Sicherheit und Funktionsfähigkeit informationstechnischer Infrastrukturen zu gewährleisten, nicht nach, wenn er gezielt dazu beitrage, Sicherheitslücken aufrechtzuerhalten, da diese auch Dritte ausnutzen könnten.[58]

---

51 Vgl. BVerfGE 141, 220 (284 f., Rn. 141); BVerfG NJW 2020, 2235 (2265, Rn. 291).

52 BVerfGE 100, 313 (361); BVerfGE 125, 260 (336).

53 Martini, in: v. Münch/Kunig (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 7. Auflage 2021, Art. 10 Rn. 159.

54 Vgl. BVerfGE 30, 1 (26 ff.); BVerfGE 100, 313 (399).

55 Huber, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, § 1 G 10 Rn. 34; Martini, in: v. Münch/Kunig (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 7. Auflage 2021, Art. 10 Rn. 171.

56 BVerfGE 100, 313 (399 f.).

57 Derin/Golla, NJW 2019, 1111 (1114 ff.); Blechschmitt, MMR 2018, 361 (365).

58 Martini, in: v. Münch/Kunig (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 7. Auflage 2021, Art. 10 Rn. 102.

Von der Quellen-TKÜ gehe eine „dysfunktionale grundrechtliche Anreizstruktur“[59] aus. Im Sinne der Effektivität der Überwachungsmaßnahmen sei es im Interesse des Staates Sicherheitslücken möglichst lange geheim zu halten. Zusätzlich befeuere das Ausnutzen von Sicherheitslücken den Markt für derartige Sicherheitslücken.[60] Das IT-Grundrecht beinhalte einen objektiven Grundrechtsgehalt, diese setze dem Gesetzgeber enge Grenzen.[61] Es wird zwar anerkannt, dass die Sicherheit der informationstechnischen Systeme und der darauf laufenden Software in erster Linie den Herstellern und Anbietern obliege und der Staat lediglich eine unterstützende Rolle innehabe. Der grundrechtliche Mindeststandard werde allerdings unterschritten, wenn eine staatliche Stelle ohne hinreichenden Grund eine Gefährdungslage bewusst aufrechterhalte oder selbst schaffe. Jedenfalls müsse der Gesetzgeber Vorgaben für ein behördliches Schwachstellenmanagement enthalten, in dem beispielsweise vorgesehen werden könnte, dass die Spähsoftware nur solche Sicherheitslücken ausnützen dürfe, die bereits bekannt seien.[62] Offen ist, ob das Bundesverfassungsgericht dieser Argumentation folgen wird. Die Streubreite der Gefahren in alle Lebensbereiche, die von unsicheren IT-Systemen ausgeht, spricht dafür, dass eine nähere Regelung zum behördlichen Umgang mit Sicherheitslücken jedenfalls zweckmäßig erscheint.

3.3.2. Zwischenergebnis

Das Bundesverfassungsgericht hat in seiner bisherigen Rechtsprechung zur Quellen-TKÜ hohe und kleinteilige Anforderungen an die Ausgestaltung der jeweiligen Regelung aufgestellt. Der Gesetzentwurf setzt viele dieser Anforderungen um. Aufgrund der Intensität des Eingriffs – gerade auch mit Blick auf die Gefährdung der allgemeinen IT-Sicherheit – bestehen aber Zweifel an der Angemessenheit der im Gesetzentwurf vorgesehenen Eingriffsschwelle.

4. Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG der Kommunikationsteilnehmer

Soweit mit der oben vorgestellten Literaturmeinung (siehe oben **3.1.**) bezüglich § 11 Abs. 1a S. 2 G 10-E ein Eingriff in den Schutzbereich des IT-Grundrechts der Kommunikationsteilnehmer angenommen wird, können verstärkte verfassungsrechtliche Bedenken bestehen.

Fraglich ist hier vor allem, ob die Eingriffsvoraussetzungen von § 3 G 10 i.V.m. § 11 Abs. 1a S. 2 G 10-E die für die Online-Durchsuchung gestellten Anforderungen an den **Rang** der geschützten **Rechtsgüter** und die **Gefahrenschwelle** erfüllen. Für eine Online-Durchsuchung müssen zumindest **tatsächliche Anhaltspunkte einer konkreten Gefahr** für **überragend wichtige Rechtsgüter**

---

59 Martini, in: v. Münch/Kunig (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 7. Auflage 2021, Art. 10 Rn. 193.

60 So die Argumentation in der Verfassungsbeschwerde gegen § 8 Abs. 12 HambVerfSChG von Golla, abrufbar unter https://freiheitsrechte.org/home/wp-content/uploads/2020/11/2020-11-20-HH_Beschwerdeschrift_ohneAdressen.pdf (letzter Abruf 17. Februar 2021), 40

61 Martini, in: v. Münch/Kunig (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 7. Auflage 2021, Art. 10 Rn. 102.

62 Verfassungsbeschwerde von Golla, (Fn. 60), 43 sowie die Argumentation in der Verfassungsbeschwerde von Strate/Ventzke gegen die § 100a StPO u.a., abrufbar unter https://www.strate.net/de/dokumentation/Sabolic-Verfassungsbeschwerde-2018-11-12-.pdf, 77 ff.

bestehen.[63] Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Diese erhöhten Anforderungen gelten auch für die Tätigkeit von Nachrichtendiensten.[64] Allerdings hält das Bundesverfassungsgericht eine gewisse Lockerung der **Wahrscheinlichkeitsmaßstäbe** unter Umständen in Bezug auf terroristische Straftaten für zulässig.[65] Eine hinreichend konkretisierte Gefahr könne danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Nach § 3 Abs. 1 G 10 i.V.m. § 11 Abs. 1a G 10-E sind bereits tatsächliche Anhaltspunkte für den Verdacht erforderlich, dass jemand eine Katalogstraftat plant, begeht oder begangen hat.[66] Hier ist jedenfalls nicht von vornherein auszuschließen, dass § 11 Abs. 1a S. 2 G 10-E nicht auch gemessen am strengeren Maßstab des IT-Grundrechts einer Verhältnismäßigkeitsprüfung standhalten könnte, zumal § 11 Abs. 1a S. 2 G 10-E den Eingriff grundsätzlich auf (gespeicherte) Kommunikationsdaten beschränkt und nicht zu einem umfassenden Ausspähen aller auf einem Endgerät gespeicherten Daten berechtigt. Mit Blick auf die gesteigerte Eingriffsintensität durch die Beeinträchtigung von IT-Systemen ist es aber auch denkbar, dass das Bundesverfassungsgericht erhöhte Anforderungen an die Eingriffsschwelle und Wertigkeit der Schutzgüter stellen wird.

5. Verletzung von Grundrechten der Anbieter von Telekommunikationsdiensten

Das **Bundesverwaltungsgericht** hat sich in seinem Urteil vom 30. Mai 2018 bereits mit der Verfassungsmäßigkeit der nach geltendem Recht bestehenden **Mitwirkungsverpflichtung** von Telekommunikationsdiensten nach § 2 Abs. 1 S. 3 G 10 auseinandergesetzt.[67] Das Gericht stellte eingangs fest, dass sich die Dienstleister **nicht auf Art. 10 Abs. 1 GG** berufen könnten.[68] Träger dieses Grundrechts seien alleine die Telekommunikationsteilnehmer, nicht aber die Übermittler dieser Kommunikation. **Ebenso wenig** greife die Mitwirkungsverpflichtung in durch **Art. 14 Abs. 1 GG** geschützte Rechtspositionen ein.[69] Es liege aber ein **Eingriff** in den **Schutzbereich** der **Berufsfreiheit** gemäß **Art. 12 Abs. 1 GG** vor.[70] Die **Mitwirkungsverpflichtung** ermögliche es der zuständigen Behörde, die personellen und sächlichen Ressourcen sowie das vorhandene Wissen des verpflich-

63 BVerfGE 120, 274 (2. Ls., 328 ff.).

64 BVerfGE 120, 274 (331).

65 BVerfGE 141, 220 (272 f., Rn. 112, 115); Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Auflage 2017, Lit. G Rn. 627.

66 Genauer Huber, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, § 3 G 10 Rn. 5 ff.

67 BVerwG, Urteil vom 30. Mai 2018, Az. 6 A 3/16, NVwZ 2018, 1476 (1482), Rn. 47 ff.

68 BVerwG, Urteil vom 30. Mai 2018, Az. 6 A 3/16, NVwZ 2018, 1476 (1479), Rn. 27.

69 BVerwG, Urteil vom 30. Mai 2018, Az. 6 A 3/16, NVwZ 2018, 1476 (1482), Rn. 47.

70 BVerwG, Urteil vom 30. Mai 2018, Az. 6 A 3/16, NVwZ 2018, 1476 (1482), Rn. 47 f.

teten Unternehmens in Anspruch zu nehmen und auf die im Zuge der Berufsausübung dort vorhandenen Telekommunikationsverkehre zuzugreifen. Sie stehe daher in engem Zusammenhang mit der Ausübung des Berufs des Telekommunikationsanbieters und lasse objektiv deutlich eine berufsregelnde Tendenz erkennen. Der Eingriff sei indes durch vernünftige Gründe des Allgemeinwohls **gerechtfertigt** und zur Erreichung des Eingriffsziels geeignet, erforderlich und verhältnismäßig im engeren Sinne.[71] Dabei stellte das Gericht darauf ab, dass die Mitwirkungspflichten für die Telekommunikationsunternehmen typischerweise **weder in technischer noch in finanzieller Hinsicht übermäßig belastend** wirkten. Gegenüber der Mitwirkungsverpflichtung bestünden deshalb **keine verfassungsrechtlichen Bedenken**. Da die bestehenden Pflichten der Diensteanbieter durch § 2 Abs. 1a G 10-E nur gezielt **inhaltlich erweitert** werden sollen, dürften diese Ausführungen **übertragbar** sein.

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) stellt zusätzlich darauf ab, durch ein massives Eindringen in die Integrität des gesamten vom Unternehmen zu verantwortenden informationstechnischen Systems werde mittelbar auch das Vertrauen in Anbieter von Softwarelösungen und Betriebssystemen unterhöhlt.[72] Dies erscheint zwar gegenüber manchen Anbietern denkbar, die gerade damit werben, dass durch die angebotene Verschlüsselung eine unangreifbare Vertraulichkeit gewährleistet werden könne. Aber es ist nicht ersichtlich, wie dieser Aspekt im Verhältnis zu dem hohen Gewicht der in Rede stehenden Rechtsgüter die Unangemessenheit eines Eingriffs in die Berufsfreiheit begründen könnte. Es kann hier nicht abgeschätzt werden, inwieweit aus den in § 2 Abs. 1a S. 1 Nr. 4 G 10-E neu geregelten Mitwirkungspflichten zur technischen Ermöglichung der Quellen-TKÜ wesentlich größere **technische, personelle oder finanzielle Belastungen** folgen, als sie nach § 2 Abs. 1 S. 3 G 10-E bereits bestehen. Wenn dies aber nicht der Fall sein sollte, spricht viel dafür, dass auch dieser Eingriff in die Berufsfreiheit **gerechtfertigt**, insbesondere verhältnismäßig wäre.

Neu ist indes die **Pflicht** der Diensteanbieter, **Zugang** zu ihren Einrichtungen **während der Geschäftszeiten** zu gewähren (§ 2 Abs. 1a S. 1 Nr. 4 G 10-E). Dies dürfte gemessen am dafür geltenden Maßstab nach **Art. 2 Abs. 1 GG**[73] unproblematisch sein.

6. Anforderungen des Trennungsprinzips

Der BfDI kritisiert, dass sich der vorliegende Gesetzentwurf schwerlich mit dem Trennungsprinzip vereinbaren lasse. Es komme zu einer unzulässigen „Befugnisparallelität“, da die Tatbestände des § 3 Abs. 1 G 10 weitgehend auch im Straftatenkatalog des § 100a Abs. 2 StPO enthalten seien.[74]

---

71 BVerwG, Urteil vom 30. Mai 2018, Az. 6 A 3/16, NVwZ 2018, 1476 (1482), Rn. 49 ff.

72 BfDI, Stellungnahme vom 4. November 2020, Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, S. 5 f., abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_Anpassung-Verfassungsschutzrecht.pdf?__blob=publicationFile&v=1 (Stand: 18. Februar 2021).

73 Siehe dazu BVerfGE 32, 54 (75 ff.).

74 BfDI, Stellungnahme vom 4. November 2020, Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, S. 4 f., abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_Anpassung-Verfassungsschutzrecht.pdf?__blob=publicationFile&v=1 (Stand: 18. Februar 2021).

Das Trennungsprinzip hat seinen Ursprung im Polizeibrief der Alliierten Militärgouverneure vom 14. April 1949. Danach war es verboten, Nachrichtendienste mit Polizeigewalt auszustatten. Der Parlamentarische Rat setzte die Vorgaben des Polizeibriefes entsprechend um und schuf damit die Grundlage für eine getrennte Behördenstruktur. Inwieweit das Trennungsgebot auch nach Wegfall des überkonstitutionellen Besatzungsrechts einen den Gesetzgeber bindenden Rechtsgrundsatz darstellt, blieb lange umstritten.[75] Das Bundesverfassungsgericht ließ die Frage, ob das Rechtsstaatsprinzip, das Bundesstaatsprinzip und der Schutz der Grundrechte es verbieten, bestimmte Behörden miteinander zu verschmelzen, ausdrücklich offen.[76] In seiner Entscheidung zur Antiterrordatei leitete es aus dem Grundrecht auf informationelle Selbstbestimmung ein zumindest **informationelles Trennungsprinzip** ab. Der Datentransfer zwischen Nachrichtendiensten und Polizeibehörden sei demnach nur ausnahmsweise unter bestimmten Voraussetzungen zulässig.[77] Aus der verfassungsgerichtlich festgestellten begrenzten Möglichkeit des Datenaustausches wird in der Literatur geschlossen, dass die Verfassung damit auch eine **hinreichende organisatorische Trennung** der Behörden verlangt und auch der **Aufgabenzuweisung** an die jeweiligen Behörden entsprechende **Grenzen** setzt.[78]

Dem Ansatz einer begrenzten Aufgabenübertragung folgend, stellen auch die Nachrichtendienstgesetze des Bundes und der Länder klar, dass von den Nachrichtendiensten **keine polizeilichen Befugnisse** ausgeübt werden dürfen.[79] Zu den polizeilichen Befugnissen zählen vor allem behördliche Handlungen mit **Zwangscharakter,** wie polizeiliche Standardmaßnahmen (z.B. Identitätsfeststellung, Sistierung, erkennungsdienstliche Maßnahmen, Festnahme, Verhaftung, Vorführung, Durchsuchung, oder Beschlagnahme).[80] Es soll im Ergebnis weder eine Geheimpolizei noch ein polizeilicher Geheimdienst entstehen.[81] Statt der Abwehr von Gefahren soll die nachrichtendienstliche Tätigkeit ausschließlich der Informationsbeschaffung dienen.[82]

Es erscheint jedoch vertretbar, sowohl Maßnahmen einer Quellen-TKÜ als auch der Online-Durchsuchung als Mittel der Informationsbeschaffung – folglich als nachrichtendienstliche Aufgabe – einzuordnen. Zwar kann einem solchen Eingriff ein gewisser Zwangscharakter nicht abgesprochen werden, da zwangsweise auf ein informationstechnisches System zugegriffen wird. Dennoch dürfte der **Schwerpunkt** dieser Maßnahme in der **Informationsbeschaffung** liegen, jedenfalls solange der Eingriff zumindest nicht auch der Manipulation des informationstechnischen Systems dienen soll.

---

75 Vgl. Nehm, NJW 2004, 3289 (3290).

76 Vgl. BVerfGE 97, 198 (217).

77 BVerfGE 133, 277 (329).

78 Bergemann, in Lisken/Denninger, Handbuch des Polizeirechts, 6. Auflage 2018, Lit. H Rn. 5.

79 Bergemann, in Lisken/Denninger, Handbuch des Polizeirechts, 6. Auflage 2018, Lit. H Rn. 5; vgl. für die Rechtslage des Bundes: § 8 Abs. 3 Bundesverfassungsschutzgesetz; § 2 Abs. 3 BND-Gesetz; § 1 Abs. 4 MAD-Gesetz; exemplarisch für die Landesebene: § 8 Abs. 7 des Verfassungsschutzgesetzes Berlin.

80 Vgl. Roth, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, § 8 BVerfSchG Rn. 48.

81 Bergemann, in Lisken/Denninger, Handbuch des Polizeirechts, 6. Auflage 2018, Lit. H Rn. 5.

82 Roth, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, § 8 BVerfSchG Rn. 48.

Das Bundesverfassungsgericht hat in seiner Entscheidung über die Zulässigkeit einer entsprechenden Regelung im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen ebenfalls nicht die Aufgabenzuweisung als solche infrage gestellt oder die Online-Durchsuchung als ausschließlich polizeiliche Maßnahme eingestuft.[83]

7. Fazit

Die Anforderungen, die das Bundesverfassungsgericht in der Vergangenheit an die Quellen-TKÜ aufgestellt hat, sind hoch und im Einzelnen sehr kleinteilig. Sie betreffen insbesondere die Ausgestaltung der Eingriffsschwelle, die Sicherstellung verfahrensrechtlicher Beschränkungen und Rechtsschutzmöglichkeiten. Der Gesetzentwurf setzt viele dieser Anforderungen um. Es bestehen allerdings begründete Zweifel daran, dass die Befugnis zum Einsatz der Quellen-TKÜ gemäß § 11 Abs. 1a G 10-E nur laufende Kommunikation umfasst. Insofern spricht viel dafür, dass sich die Regelung auch am strengeren Maßstab für die Online-Durchsuchung zu messen hat. Es lässt sich noch nicht abschließend abschätzen, welchen Maßstab das Bundesverfassungsgericht hier anlegen würde. Aufgrund der hohen Eingriffsintensität gerade auch mit Blick auf die allgemeine IT-Sicherheit bleiben Zweifel an der Angemessenheit der im Gesetzentwurf vorgesehenen Eingriffsschwelle bestehen. Die Vereinbarkeit von § 2 Abs. 1a G 10-E mit der Berufsfreiheit der Diensteanbieter ist abhängig davon, ob aus den neuen Mitwirkungspflichten wesentlich größere technische, personelle oder finanzielle Belastungen folgen. Dies kann hier nicht abschließend beurteilt werden. Wenn dies aber nicht der Fall sein sollte, spricht viel dafür, dass dieser Eingriff in die Berufsfreiheit gerechtfertigt, insbesondere verhältnismäßig wäre. Die Regelung dürfte mit dem Trennungsprinzip vereinbar sein.

***

83 Vgl. BVerfGE 120, 274 (329 ff.).