15. Mai 2021

Dr. Benjamin Rusteberg
z. Zt. Vertreter des Lehrstuhls für Öffentliches Recht,
insb. Kirchenrecht und Staatskirchenrecht
Georg-August-Universität Göttingen
Goßlerstraße 11
37073 Göttingen

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)844 D

Stellungnahme

zur Vorbereitung der öffentlichen Anhörung des

Ausschusses für Inneres und Heimat des Deutschen Bundestages

zum

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts

BT-Drucksachen 19/24785, 19/24900

Aufgrund der überaus knapp bemessenen Zeit für die Vorbereitung der Anhörung kann im Folgenden nicht zu sämtlichen Punkten und allen Anträgen Stellung genommen werden. Deshalb beschränken sich die folgenden Ausführungen auf den Gesetzesentwurf der Bundesregierung und bei diesem auf diejenigen Punkte, die als besonders relevant angesehen werden.

A. Vorbemerkungen

Die Nachrichtendienste werden in der Bundesrepublik traditionell insbesondere von der Polizei aber auch von den Strafverfolgungsbehörde und von anderen Verwaltungsbehörden abgegrenzt, die über außenwirksame Exekutivbefugnissen verfügen. Man spricht hier von dem sogenannten Trennungsgebot.

Insbesondere vor dem Hintergrund dieses Trennungsgebots kann jedoch die Frage, wie das Verhältnis der Nachrichtendienste – insbesondere der Verfassungsschutzämter – zu den übrigen Sicherheitsbehörden ausgestaltet ist und welche Funktion die Nachrichtendienste in der bundesdeutschen Sicherheitsarchitektur einnehmen, nach wie vor nicht wirklich befriedigend beantwortet werden kann.

Nach § 1 Abs. 1 BVerfSchG dient der Verfassungsschutz dem Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes und der Länder. Aufgabe der

Verfassungsschutzbehörden soll gem. § 3 Abs. 1 BVerfSchG die Sammlung und Auswertung von Informationen über eben solche Bestrebungen sein, die sich gegen die freiheitlich demokratisch Grundordnung richten bzw. Bestand und Sicherheit des Bundes und der Länder gefährden.

Das Sammeln von Informationen allein, schützt aber weder den Staat noch die Verfassung. Informationen zu sammeln ist kein Selbstzweck. Vielmehr kommt es darauf an, was mit diesen Informationen geschehen soll.

Das Bundesverfassungsschutzgesetz enthält zu dieser Frage bemerkenswerterweise keinerlei Angaben. In einigen Landesverfassungsschutzgesetzen wird die Aufgabe hingegen ausdrücklich dahingehend bestimmt, dass die Verfassungsschutzämter es den zuständigen Stellen zu ermöglichen haben, „rechtzeitig die erforderlichen Maßnahmen zur Abwehr von Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder zu treffen."[1]

Auch diese Normierung wirft jedoch mehr Fragen auf, als sie beantwortet. So bleibt weiterhin unbenannt, welches diese Stellen sind, die die erforderlichen Abwehrmaßnahmen zu treffen haben.

Sollen dies gerade die Behörden sein, die über Exekutivbefugnisse verfügen, stellt sich die Frage, was vom Trennungsgebot bleibt, wenn die Aufgabe der Verfassungsschutzbehörden in erster Linie darin besteht, diesen Informationen zuzuliefern. Zugleich ist zu fragen, warum diese Aufgabe dann nicht einfach von den polizeilichen Staatsschutzabteilungen übernommen wird, deren Befugnisse zur Informationserhebung hinter denen des Verfassungsschutzes keineswegs zurückstehen.[2]

Legt man demgegenüber bei der Nutzung der Informationen den Schwerpunkt auf die Information der jeweiligen Bundes- bzw. Landesregierung stellt sich namentlich bei den Verfassungsschutzbehörden – beim BND mag dies in gewissem Rahmen anders sein – die Frage, ob für diese Aufgabe wirklich ein umfangreiches Arsenal an Befugnissen zur heimlichen Überwachung vonnöten ist. Dies gilt umso mehr, wenn man die Kosten in Betracht zieht, den der Einsatz derartiger Mittel für die Arbeit der übrigen Sicherheitsbehörden und die Allgemeinheit mit sich bringen kann.

Diese Problematik der nach wie vor ungeklärten Aufgabe des Verfassungsschutzes und der Rolle, die ihm in der bundesdeutschen Sicherheitsarchitektur zukommen soll, zieht sich auch durch den vorliegenden Gesetzesentwurf:

- § 4 Abs. 1 BVerfSchG-E bekräftigt die Rolle des Bundesamtes für Verfassungsschutz (BfV) noch weiter, indem anstelle von Strukturen verstärkt als gefährlich angesehene Einzelpersonen beobachtet werden sollen;
- § 11 Abs. 1a G10-E will den Nachrichtendiensten zusätzliche Befugnisse zu heimlichen Überwachungsmaßnahmen einräumen, die bislang Polizei- und Strafverfolgungsbehörden

[1] § 2 II 2 HessVSG; vgl. § 3 I BW ; § 1 II Th VSG.

[2] Vgl. hierzu R. Poscher/B.Rusteberg, Die Aufgabe des Verfassungsschutzes, KJ 2014, 57 ff.; dies., Ein Kooperationsverwaltungsrecht des Verfassungsschutzes?, in: Dietrich/Gärditz/Graulich/Gusy/Warg (Hrsg.), Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S.145 ff.; B. Rusteberg, Informationsherrschaft durch Polizei und Nachrichtendienste, in: Kulick/Goldhammer (Hrsg.), Der Terrorist als Feind?, 2020, S. 215 ff.

vorbehalten waren; dennoch sollen an den Einsatz derartiger Maßnahmen durch die Nachrichtendienste geringere Anforderungen zu stellen sein als bei den letztgenannten;

- § 2 Abs. 1a u. 1b G10-E soll den Nachrichtendiensten umfassende tatsächliche Zugriffs- und Manipulationsmöglichkeiten des gesamten Datenverkehrs im Bereich der Telekommunikation einräumen, die weit über das hinausgehen, was Polizei- und Strafverfolgungsbehörden möglich ist.

B. Artikel 1 – Änderung des Bundesverfassungsschutzgesetzes: Nummer 1 - § 4 Abs. 1 BVerfSchG-E

Geltende Gesetzeslage	Gesetzesentwurf	Neufasssung
§ 4 Begriffsbestimmungen (1) [1][…] [2]Für einen Personenzusammenschluß handelt, wer ihn in seinen Bestrebungen nachdrücklich unterstützt. [3]Voraussetzung für die Sammlung und Auswertung von Informationen im Sinne des § 3 Abs. 1 ist das Vorliegen tatsächlicher Anhaltspunkte. [4]Verhaltensweisen von Einzelpersonen, die nicht in einem oder für einen Personenzusammenschluß handeln, sind Bestrebungen im Sinne dieses Gesetzes, wenn sie auf Anwendung von Gewalt gerichtet sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut dieses Gesetzes erheblich zu beschädigen.	**1. § 4 Absatz 1 wird wie folgt geändert:** a) Nach Satz 2 werden die folgenden Sätze eingefügt: „Bestrebungen im Sinne des § 3 Absatz 1 können auch von Einzelpersonen ausgehen, die nicht in einem oder für einen Personenzusammenschluss handeln. In diesem Fall gilt Satz 1 mit der Maßgabe, dass die Verhaltensweise der Einzelperson darauf gerichtet sein muss, die dort genannten Ziele zu verwirklichen.“ b) Der neue Satz 6 wird aufgehoben.	**§ 4 Begriffsbestimmungen** (1) [1][…] [2]Für einen Personenzusammenschluß handelt, wer ihn in seinen Bestrebungen nachdrücklich unterstützt. [3]Bestrebungen im Sinne des § 3 Absatz 1 können auch von Einzelpersonen ausgehen, die nicht in einem oder für einen Personenzusammenschluss handeln. [4]In diesem Fall gilt Satz 1 mit der Maßgabe, dass die Verhaltensweise der Einzelperson darauf gerichtet sein muss, die dort genannten Ziele zu verwirklichen. [5]Voraussetzung für die Sammlung und Auswertung von Informationen im Sinne des § 3 Abs. 1 ist das Vorliegen tatsächlicher Anhaltspunkte.

I. Gesetzesbegründung

Nach Art. 1 Nr. 1 des Entwurfs eines Gesetzes zur Anpassung des Verfassungsschutzrechts soll § 4 Abs.1 BVerfSchG dahingehend geändert werden, dass zukünftig die Beobachtung von Einzelpersonen unter denselben Voraussetzungen möglich ist, wie die Beobachtung von Personenzusammenschlüssen. Letztere bilden bislang den primären Gegenstand der Beobachtungstätigkeit, während Einzelpersonen gem. § 4 Abs. 1 S. 4 BVerfSchG, soweit sie nicht in einem oder für einen Personenzusammenschluss handeln, nur dann relevante Bestrebungen und damit ein zulässiges Beobachtungsobjekt darstellen, wenn ihre Verhaltensweisen „auf Anwendung von Gewalt gerichtet sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut dieses Gesetzes erheblich zu beschädigen“.

Begründet wird die vorgesehene Änderung damit, dass „unter den Bedingungen der digitalen Moderne und Erkenntnissen zu Radikalisierungsverläufen“ nicht daran festgehalten werden könne, dass „bei Bestrebungen einerseits von Personenzusammenschlüssen und andererseits von Einzelpersonen grundsätzlich unterschiedlichen Bedrohungseinschätzung“ bestünden.[3] Beispielsweise eröffneten soziale Medien Einzelpersonen eine enorme Wirkungsbreite für Agitation und Hassbotschaften. Zudem erfordere die „Frühwarnfunktion des Verfassungsschutzes gerade nach den Anschlägen in Halle am 9. Oktober 2019 und Hanau am 19. Februar 2020 angesichts eruptiver Radikalisierungsverläufe von Einzelpersonen, Extremisten bereits im Vorfeld militanter Handlungen besser in den Blick nehmen zu können“. Die neue Regelung trage dem Rechnung, sehe dabei aber eine besondere Würdigung des Einzelfalls vor, „indem – anders als bei Personenzusammenschlüssen – zu Einzelpersonen ein Entschließungsermessen auszuüben ist, bei dem im Kern die Schutzgutrelevanz des Sachverhalts – auch in seinem Entwicklungspotenzial – zu beurteilen“ sei. Eine solche Risikoabschätzung sei bereits im Rahmen des personenbezogenen Bearbeitungsansatzes der Sicherheitsbehörden methodisch etabliert, etwa bei der sicherheitsbehördlichen Priorisierung in der Gefährderbearbeitung.

II. Rechtliche Bewertung

Die für die vorgesehene Gesetzesänderung gegebene Begründung kann nicht überzeugen. Insbesondere sprechen die angeführten Anschlägen von Halle und Hanau keineswegs für die Notwendigkeit einer derartigen Änderung.

Dies folgt schon daraus, dass in beiden Fällen die Verhaltensweise gerade auf die „Anwendung von Gewalt“ gerichtet waren, und somit auch bereits nach der geltenden Rechtslage in den Aufgabenbereich des Verfassungsschutzes fielen. Auch nach der geltenden Rechtslage ist es nach dem klaren Wortlaut von § 4 Abs. 1 S. 3 u. 4 BVerfSchG keineswegs so, dass die zu beobachtende Einzelperson etwaige Gewalthandlungen bereits begangen haben muss. Vielmehr reichen Anhaltspunkte aus, dass sie entsprechende Absichten verfolgt.

Die im Entwurf vorgesehene Änderung erweist sich damit in erster Linie als Ausdruck des bereits angesprochenen Bemühens, die Aufgabe des Verfassungsschutzes vom Ziel einer Strukturaufklärung weg, hin zu einer Zuständigkeit als besondere Gefahrenabwehrbehörde zu entwickeln. Damit vertiefen sich freilich die oben angesprochenen Zweifel an dem Eigenwert, der einer derartigen Behörde gegenüber den ebenfalls über umfassende Möglichkeiten der Informationsvorsorge verfügenden Polizeien zukommt. Zudem stellt eine solche Rolle des Verfassungsschutzes in letzter Konsequenz das Trennungsgebot in Frage. Ohne dieses verschwinden aber auch jegliche Argumente, warum die Anforderungen an die Eingriffsschwellen bei Überwachungsmaßnahmen der Nachrichtendienste nach dem G10 gegenüber Maßnahmen nach den Polizeigesetzen und der StPO abgesenkt werden sollten.

Dabei geht die Entwurfsbegründung in nicht nachvollziehbarerweise von der Existenz eines Entschließungsermessens des BfV nach § 4 Abs. 1 BVerfSchG-E aus.[4] Soweit die Entwurfsbegründung diesbezüglich auf die Notwendigkeit einer Risikoabschätzung verweist, die „bereits im Rahmen des personenbezogenen Bearbeitungsansatzes der Sicherheitsbehörden methodisch etabliert“ sei,[5] drängt

[3] BT-Drs. 19/24785, S. 17.
[4] BT-Drs. 19/24785, S. 17; dazu 19(4)844 A - Stellungnahme Prof. Dr. Matthias Bäcker, S. 6.
[5] BT-Drs. 19/24785, S. 17.

sich der Verdacht auf, dass die Gesetzesänderung in erster Linie zur nachträglichen Legitimation einer bereits jetzt contra legem eingeübten behördlichen Praxis dienen soll.

C. Artikel 5 – Änderung des Artikel 10-Gesetzes

I. Nummer 7 lit. a) - § 11 Abs. 1a G10-E

7. § 11 wird wie folgt geändert:

a) Nach Absatz 1 werden die folgenden Absätze 1a und 1b eingefügt:

„(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.

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. Bei jedem Einsatz sind zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt. […]

1. Übersicht

a) Gesetzesbegründung

Ausweislich der Entwurfsbegründung soll mit Artikel 5 Nr. 7 lit. a) eine Aufklärungslücke geschlossen werden, die sich aufgrund der gegenwärtigen Entscheidungspraxis der G10-Kommission bei sog. Messengerdiensten ergebe, die technisch aus dem Speicherplatz des Endgeräts – unverschlüsselt –

ausgelesen werden müssten („ruhende Kommunikation“). Diese Lücke werde mit der Regelung in Absatz 1a Satz 2 geschlossen. Diese orientiere sich an dem Modell der Strafprozessordnung (§ 100a Abs. 1 S. 2 u.3 sowie Absatz 5 und 6).[6]

b) Vergleich mit bestehenden Regelungen

§ 11 G10 - Neufassung	**§ 100a StPO**	**§ 51 BKAG**
(1a)	(1) [1] […]	(2)
[1]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.	[2]Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen.	[1]Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn […]
[2]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. […]	[3]Auf dem informationstechnischen System des Betroffenen 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.	

[6] BT-Drs. . 19/24785, S. 22 f.

(1a) […] [3]Bei den Maßnahmen nach den Sätzen 1 und 2 ist technisch sicherzustellen, dass	(5) Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass	(2) […] wenn
1. ausschließlich überwacht und aufgezeichnet werden können:	1. ausschließlich überwacht und aufgezeichnet werden können:	1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird und
a) die laufende Kommunikation (Satz 1) und	a) die laufende Telekommunikation (Absatz 1 Satz 2), oder	2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.
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),	b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),	§ 49 Absatz 2 gilt entsprechend. § 49 bleibt im Übrigen unberührt.
		§ 49 BKAG
2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,	2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und	(2) Es ist technisch sicherzustellen, dass 1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.	3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.	2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.
[4]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.	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.	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.

[5]Bei jedem Einsatz sind zu protokollieren:	(6) Bei jedem Einsatz des technischen Mittels sind zu protokollieren	→ **§ 82 BKAG**
1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,	1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,	
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,	2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,	
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und	3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und	
4. die Organisationseinheit, die die Maßnahme durchführt.	4. die Organisationseinheit, die die Maßnahme durchführt.	

Wie bereits die Gesetzesbegründung deutlich macht, orientiert sich die vorgeschlagene Regelung an § 100a Abs. 1 S. 2 u. 3, Abs. 5 u. 6 StPO. Diese wurden mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017[7] in die Strafprozessordnung eingefügt.

Insbesondere in der Rechtsfolge stimmen § 100a Abs. 1 S. 3 StPO und § 11 Abs.1a S. 2 G10-E dahingehend überein, dass sie den Eingriff in ein informationstechnisches System nicht nur für die Überwachung der laufenden Telekommunikation, sondern auch für Inhalte und Umstände der Kommunikation zulassen, die ab dem Zeitpunkt der Anordnung gespeichert wurden, wenn diese hypothetisch auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

Beide Regelungen gehen damit insbesondere über § 51 Abs. 2 BKAG hinaus, der lediglich die Überwachung und Aufzeichnung laufender Telekommunikation erlaubt, wenn dafür mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird.

2. Verfassungsrechtliche Maßstäbe

Die auf § 11 Abs. 1a G10-E anwendbaren verfassungsrechtlichen Maßstäbe unterscheiden sich signifikant, je nachdem ob in der Regelung ein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG enthalten ist, oder sie sich auf Eingriffe in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG bzw. das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG beschränkt.

[7] BGBl. 2017 I, S. 3202 ff.

a) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt vor einem Zugriff auf informationstechnische Systeme zur geheimen Durchführung von Online-Durchsuchungen, mit denen private, von den Betroffenen auf eigenen oder vernetzten fremden Computern (wie etwa der sogenannten Cloud) abgelegte oder hinterlassene Daten erhoben werden können und die es ermöglichen, das Verhalten der Betroffen im Netz nachzuvollziehen.[8]

Nach der Rechtsprechung des Bundesverfassungsgerichts trägt die Verfassung mit dieser eigenständigen Ausprägung des allgemeinen Persönlichkeitsrechts der heute weit in die Privatsphäre hineinreichenden Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung Rechnung. Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergebe, sei ein Eingriff in dieses Grundrecht von besonderer Intensität und seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar.[9]

Für Eingriffe in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gelten deshalb besonders strenge Anforderungen: Insbesondere müssen die gesetzlichen Ermächtigungsgrundlagen vorsehen, dass mindestens tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen.[10]

b) Fernmeldegeheimnis, Art. 10 Abs. 1 GG

Der Schutz des Fernmeldegeheimnisses bezieht sich nach der Rechtsprechung des Bundesverfassungsgerichts auf alle mittels der Fernmeldetechnik ausgetauschten Informationen und umfasst sowohl den Kommunikationsinhalt als auch die Kommunikationsumstände. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt der über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Information zu verschaffen.[11] Eines besonderen grundrechtlichen Schutzes bedarf es aufgrund der spezifischen Verletzlichkeit, sobald Informationen unter Einschaltung eines Kommunikationsmittlers über eine Distanz hinweg ausgetauscht werden.[12]

Dabei hat das Bundesverfassungsgericht zwar auch Zugriffe „am Endgerät“ in den Schutzbereich des Art. 10 Abs. 1 GG einbezogen. Nicht mehr durch Art. 10 Abs. 1 GG geschützt sind aber Zugriffe auf ehemalige oder zukünftige Kommunikationsinhalte oder Kommunikationsumstände im Machtbereich

[8] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220, Rn. 209; BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274, Rn. 201 ff.
[9] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 210.
[10] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 212; BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274, Rn. 242 ff.
[11] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, BVerfGE 113, 348-392, Rn. 82.
[12] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473), m.w.N.

der Kommunikationspartner: Sobald der Kommunikationsinhalt beim Empfänger angekommen ist, endet der Schutz des Art. 10 Abs. 1 GG.[13]

Ein Eingriff in das Fernmeldegeheimnis liegt demnach vor, wenn staatliche Stellen sich ohne Zustimmung der Beteiligten Kenntnis von dem Inhalt oder den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen.[14]

Für die Eingriffsintensität einer konkreten Maßnahme bedeutsam ist u.a. die Streubreite der Eingriffe, insofern nicht nur potenziellen Störer oder Straftäter erfasst werden, sondern alle, mit denen diese in dem betreffenden Zeitraum Telekommunikationsverbindungen nutzen.[15] Zur weiteren Intensivierung des Eingriffs trägt bei, dass die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertraulichkeit ausgesetzt sind.[16] Noch weitere werde die Schwere des Eingriffs durch eine Datenerhebung im Vorfeld erhöht, da hieraus die Möglichkeit einer Verwendung der erhobenen Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken resultiere.[17]

Für die Rechtfertigung setzen Eingriffe in das Fernmeldegeheimnis grundsätzlich hinreichend gewichtige Schutzgüter sowie ausreichend konkretisierte Eingriffsschwellen voraus.[18]

c) Einordnung und Voraussetzungen der sog. Quellen-TKÜ

aa) Schutzbereichsausnahme

Der Begriff „Quellen-TKÜ“ bezeichnet die Telekommunikationsüberwachung durch Infektion des verwendeten Endgeräts mit einer Überwachungssoftware, dem sog. Trojaner. Sie bezieht sich damit insbesondere auf Telefongespräche, die nicht über klassische Telefonverbindungen, sondern über das Internet geführt werden, aber etwa auch auf E-Mails, Chats und Messengerdienste oder die Inhalte aufgerufener WWW-Seiten. Der technische Nutzen der Quellen-TKÜ besteht darin, dass die Daten in den beteiligten Rechnern oder Smartphones regelmäßig noch vor dem Versand der Daten über das Internet verschlüsselt werden. Ein erfolgversprechender Zugriff auf solche Kommunikation ist daher regelmäßig nicht durch Zugriff entlang der Übertragungsstrecke, sondern nur noch durch das „Anzapfen“ eines der beteiligten Endgeräte möglich, um dort die noch bzw. bereits wieder entschlüsselten Daten „an der Quelle“ abgreifen zu können.[19]

Das Bundesverfassungsgericht hat diese sog. Quellen-TKÜ privilegiert, indem es für sie eine Schutzbereichsausnahme vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vorgenommen hat: Obwohl sich die Quellen-TKÜ gerade dadurch auszeichnet, dass bei ihr verdeckte Eingriffe in informationstechnische Systeme notwendig sind, soll sie grundsätzlich keinen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und

---

[13] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473), m.w.N.

[14] BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 –, BVerfGE 129, 208-268, Rn. 198 f.

[15] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, BVerfGE 113, 348-392, Rn. 142.

[16] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, BVerfGE 113, 348-392, Rn. 143.

[17] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, BVerfGE 113, 348-392, Rn. 146.

[18] B. Rusteberg, Die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz, KritV 2017, 24 (30).

[19] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 f.

Integrität informationstechnischer Systeme darstellen, sondern sich ausschließlich nach den Vorgaben richten, die auch sonst für die Telekommunikationsüberwachung gelten.[20]

Ausdrückliche Voraussetzung ist insofern jedoch, dass die hierfür notwendigen Eingriffe in das informationstechnische System rechtlich voraussetzen und technisch sicherstellen, dass eine Überwachung nur für die laufende Telekommunikation erfolgt. Andernfalls komme allein ein Vorgehen nach den Vorschriften in Betracht, die für einen Eingriff in informationstechnische Systeme gelten.[21] Maßgeblich sei insoweit, „ob das Programm so ausgestaltet ist, dass es - hinreichend abgesichert auch gegenüber Dritten - den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern des Bundeskriminalamts inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht." Hingegen komme es nicht darauf an, „ob durch eine technisch aufwendige Änderung des Überwachungsprogramms selbst – sei es durch die Behörde, sei es durch Dritte – dessen Begrenzung auf eine Erfassung der laufenden Telekommunikation aufgehoben werden" könne.[22]

Für die Gültigkeit der gesetzlichen Ermächtigungsgrundlage soll nach der Rechtsprechung des Bundesverfassungsgerichts dabei unerheblich sein, inwieweit tatsächlich technische Maßnahmen existieren, die sicherstellen, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird. Diese Frage betreffe „die Anwendung der Norm, nicht aber ihre Gültigkeit". Sollten diese Anforderungen zum jeweiligen Zeitpunkt nicht erfüllbar sein, laufe die Vorschrift schlicht leer.[23]

bb) Laufende Kommunikation

Die Schutzbereiche beider Grundrechte sind insoweit komplementär angelegt: Sobald die engen Grenzen der „laufenden Kommunikation" überschritten sind, also insbesondere auf bereits übermittelte oder zukünftig (möglicherweise) einmal zu übermittelnde Daten zugegriffen werden soll, und damit der verfassungsrechtlich zulässige Anwendungsbereich der Quellen-TKÜ verlassen wird, stellt sich der Eingriff ohne weiteres als Online-Durchsuchung dar.[24]

Datenverarbeitungsvorgänge im alleinigen Machtbereich eines der beteiligten Kommunikationspartner können dabei nur so lange als Teil der laufenden Kommunikation angesehen und damit vom Schutzbereich des Art. 10 Abs. 1 GG erfasst werden, als sie noch als Teil einer Verwendung als „Telefonie-Endgerät" angesehen werden können. Dies umfasst allein solche technischen Vorgänge, die unmittelbar der Übergabe von Kommunikationsinhalten an einen Informationsmittler dienen und sich somit als integraler Bestandteil der Telekommunikation im Sinne des Fernmeldegeheimnisses darstellen.[25] Nicht umfasst sind hingegen insbesondere solche Vorgänge im Machtbereich eines Kommunikationspartners, die lediglich der Vorbereitung von Daten auf eine

[20] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274, Rn. 190; Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der QuellenTelekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473).

[21] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 234.

[22] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 234.

[23] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 234.

[24] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473).

[25] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473).

mögliche spätere Kommunikation oder der Weiterverarbeitung bereits empfangener Daten, also früherer Kommunikation, dienen.[26]

Laufende Telekommunikation umfasst damit Datenverarbeitungsvorgänge, die sich entweder im Herrschaftsbereich eines Informationsmittlers oder im Herrschaftsbereich eines der Kommunikationspartner abspielen, dabei aber unmittelbar – d.h. ohne weitere Zwischenschritte – der Übergabe von Kommunikationsinhalten an einen Informationsmittler dienen.[27]

3. Schutzbereichszuordnung der Ermächtigung des § 11 Abs. 1a G10

Gesetzessystematisch bestimmt sich der Anwendungsbereich des § 11 G10 nach § 1 Abs. 1 G10. Die materiellen Voraussetzungen einer derartigen Beschränkung des Fernmeldegeheimnisses im Einzelfall ergeben sich aus den §§ 3 bis 3b G10, die formellen Voraussetzungen, soweit sie nicht in § 11 G10 geregelt sind, aus den §§ 9 ff. G10.

a) Begriff der „Telekommunikation“

Gem. § 1 Abs. 1 Nr. 1 G10 sind die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen.

Zur Konkretisierung des Begriffs der Telekommunikation wird insoweit grundsätzlich auf § 3 Nr. 22 TKG zurückgegriffen. Nach der dortigen Legaldefinition ist „Telekommunikation“ der technische Vorgang des Aussendens von Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Damit werden alle Formen der Nachrichtenübermittlung unter Raumüberwindung in nicht-körperlicher Weise mittels technischer Einrichtungen erfasst. Hierzu zählen u.a. die Telefonie über Festnetz oder Mobilfunk, der SMS-Versand und der E-Mail-Verkehr sowie weitere Anwendungen des Internets.[28]

Das Überwachen und Aufzeichnen dieser mittels Telekommunikationsanlagen übermittelten Daten stellt damit grundsätzlich einen Eingriff in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG dar.

b) Abgrenzung laufender von abgeschlossener Telekommunikation

aa) § 11 Abs. 1a S. 1, 3 Nr. 1 lit. a) G10-E

§ 11 Abs. 1a S. 1 G10-E ermächtigt zunächst dazu, die Überwachung und Aufzeichnung der laufenden Telekommunikation in der Art und Weise vorzunehmen, „dass in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen wird, wenn dies notwendig ist, um die Überwachung und

---

[26] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (474): Insoweit verlaufe die verfassungsrechtliche Abgrenzung parallel zur technischen Abgrenzung zwischen Inhalts- und Transportverschlüsselung; vgl. auch M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra 24/2020, 1 (6).

[27] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der QuellenTelekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473 f.).

[28] F. Roggan, G10, 2. Aufl. 2018, G 10 § 1 Rn. 12; vgl. zum ähnlich weiten Begriff der Telekommunikation in § 100a StPO BVerfG, Nichtannahmebeschluss vom 06. Juli 2016 – 2 BvR 1454/13 –, juris; BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018 – 2 BvR 2377/16 –, juris, Rn. 42.

Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen“. Gem. § 11 Abs. 1a S. 3 Nr. 1 lit. a) G10-E ist überdies technisch sicherzustellen, dass ausschließlich die laufende Kommunikation überwacht und aufgezeichnet werden kann. Zudem dürfen gem. § 11 Abs. 1a S. 3 Nr. 2 u. 3 G10-E 2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und die vorgenommenen Veränderungen müssen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Insoweit entspricht die Regelung den dargestellten Voraussetzungen, um als sog. Quellen-TKÜ eine Schutzbereichsausnahme aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu erfahren.

Irritierend ist jedoch bereits an dieser Stelle die Formulierung, die § 11 Abs. 1a S. 1 G10-E – insoweit abweichend von § 100a Abs. 1 S. 2 StPO – verwendet, wonach die Überwachung und Aufzeichnung der laufenden Telekommunikation, *die nach dem Zeitpunkt der Anordnung übertragen worden ist*, in der beschriebenen Art und Weise erfolgen darf. Nach der Systematik der Sätze 1 u. 2 – siehe dazu sogleich – ist davon auszugehen, dass Satz 1 sich ausschließlich auf die laufende Übertragung beziehen soll. Würde Satz 1 hingegen so gelesen, dass auch er sich auf bereits abgeschlossene Übertragungen bezieht, wäre auch er als Ermächtigung nicht bloß zur Quellen-TKÜ, sondern zur Online-Durchsuchung zu qualifizieren.

Insofern ist eine dies klarstellende Formulierung erforderlich, etwa dass eine Überwachung und Aufzeichnung der laufenden Telekommunikation, die nach dem Zeitpunkt der Anordnung übertragen *wird*, in der beschriebenen Art und Weise erfolgen darf.

bb) § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E

Gem. § 11 Abs. 1a S. 2 G10-E soll es den Nachrichtendiensten zudem erlaubt sein, *ab dem Zeitpunkt der Anordnung gespeicherte* Inhalte und Umstände der Kommunikation auf dem informationstechnischen System des Betroffenen zu überwachen und aufzuzeichnen, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

Dem korrespondierend ist gem. § 11 Abs. 1a S. 3 Nr. 1 lit. b) G10-E auch technisch lediglich sicherzustellen, dass neben der laufenden Kommunikation nur 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*, überwacht und aufgezeichnet werden.

Damit geht aber bereits der Wortlaut des Gesetzentwurfs davon aus, dass mit der Ermächtigung des § 11 Abs. 1a S. 2 G10-E die Überwachung über die laufende Kommunikation hinaus ausgedehnt werden soll. Insoweit bewegt sich die Maßnahme jedoch außerhalb der vom Bundesverfassungsgericht vorgenommenen Schutzbereichsausnahme und stellt nicht mehr nur einen Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG dar, sondern greift in den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein.

Diese Bewertung deckt sich im Übrigen mit der ganz herrschenden Meinung der Literatur zur Regelung des § 100a Abs. 1 S. 3 StPO, der § 11 Abs. 1a S. 2 G10-E nachgebildet ist.[29]

[29] Siehe etwa BeckOK IT-Recht/Brodowski, 1. Ed. 1.9.2020, StPO § 100a Rn. 10: „Ohnehin verkennt diese Regelung, dass die gespeicherten Daten – jedenfalls in der Regel – nicht mehr Art. 10 GG unterliegen, sodass der Eingriff am Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) zu messen ist, zu dem § 100a nicht legitimiert."
Ders./U. Sieber, in: Hoeren/Sieber/Holznagel MMR-HdB, 54. EL Oktober 2020, Teil 19.3 Strafprozessrecht, Rn. 151: „Besonders kritisch zu beurteilen ist schließlich die Erweiterung in § 100 a Abs. 1 Satz 3 StPO, der zufolge auch mit technischen Mitteln retrospektiv „Inhalte und Umstände der Telekommunikation […] überwacht und aufgezeichnet werden [dürfen], wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können" (hypothetische Kommunikationsinhalte). Diese sind gem. § 100 a Abs. 5 Nr. 1 lit. b StPO auf Daten begrenzt, „die ab dem Zeitpunkt der Anordnung nach § 100 e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können", wenn sie denn nicht verschlüsselt worden wären. Indessen ist es bereits aus forensischer Sicht sehr zweifelhaft, ob sich im Nachhinein treffsicher diese (und nur diese) Inhalte und Umstände rekonstruieren lassen. Zudem geben diese unter Umständen bei nur teilweise möglicher Rekonstruktion ein unvollständiges Bild wieder. Am gravierendsten ist jedoch, dass der anwendbare Grundrechtsmaßstab verkannt wurde: Es wird auf Daten zugegriffen, die – eventuell – in der Vergangenheit zwar Gegenstand von Telekommunikation waren, die aber jetzt nicht mehr dem Schutz des Art. 10 GG unterliegen, sondern dem (strengeren) Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG). Hinzu kommt, dass durch die weite Fassung der Zieldaten möglicherweise eine noch umfassendere Suche nach solchen Daten auf dem infiltrierten Computersystem möglich wird. Es sprechen deswegen gute Gründe für eine – zumindest teilweise – Verfassungswidrigkeit von § 100 a Abs. 1 Satz 3 StPO."
M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ 2020, 1803: „Die StPO erlaubt darüber hinaus, im Rahmen der Quellen-TKÜ auf gespeicherte Kommunikation zuzugreifen, wenn diese zuvor Gegenstand eines Übertragungsvorgangs war (vgl. § 100 a I 3 StPO). Sie gestattet damit rückwirkend den Zugriff auf vergangene Kommunikationsdaten, namentlich solche, die eine Zielperson zwischen Anordnungszeitpunkt und Inbetriebnahme der Überwachungssoftware übertragen oder erhalten hat (vgl. § 100 a V 1 Nr. 1 b StPO; BT-Drs. 18/12785, 52 f.). Damit überschreitet die Norm die kritische Grenze zur Online-Durchsuchung; der Eingriff muss sich am so genannten IT-Grundrecht messen. Die Vorschrift ist daher verfassungswidrig." Ausf. auch dies., NVwZ – Extra 24/2020, 1 (7 f.).
S. Großmann, Telekommunikationsüberwachung und Online-Durchsuchung, JA 2019, 241 (243): „Überzeugen kann dies nicht: Die Betroffenheit eines Grundrechts bemisst sich nach der Art des Eingriffs und kann nicht rückwirkend durch das durch die Maßnahme erlangte Ergebnis relativiert werden. Das Auslesen und Aufzeichnen gespeicherter Kommunikationsinhalte setzt ein Eindringen und Durchsuchen des gesamten Systems nach relevanten Kommunikationsinhalten voraus. Aufgrund der enormen Sensibilität der auf informationstechnischen Geräten gespeicherten Daten wiegt ein Eingriff hierin stets erheblich schwerer als ein bloßes „Anzapfen" externer Leitungen. Es verwundert sehr, wie leichtfertig der Gesetzgeber den vom BVerfG durch das IT-Grundrecht geschaffenen Schutzbereich ignoriert."
F. Freiling/C. Safferling/C. Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung, JR 2018, 9 (21): „Die vom BVerfG der Entscheidung zugrunde gelegte Parallelität zwischen TKÜ und Quellen-TKÜ trägt aber nur soweit, wie tatsächlich laufende Telekommunikation überwacht wird. Das betonen die Verfassungsrichter auch hinsichtlich der Kernbereichsnähe der TKÜ. Bei Daten nach § 100a Abs. 5 Nr. 1 b StPO n.F. (Daten, die nach Anordnung aber vor tatsächlichem technischen Zugriff gespeichert werden) versagt demnach die Eingriffsrechtfertigung durch das BVerfG. Hier handelt es sich tatsächlich um eine (beschränkte) Online-Durchsuchung."
T. Singelnstein/B. Derin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, NJW 2017, 2646 (2648): „Auch bei einem derart engen Verständnis ist die Regelung gleichwohl nicht mit der Rechtsprechung des BVerfG in Einklang zu bringen. Dieser zufolge markiert die Beschränkung auf laufende Kommunikation in Abgrenzung zu gespeicherten Daten gerade die Grenze zwischen Art. 10 I GG und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die Vorschrift ist daher nicht mehr nur am Fernmeldegeheimnis, sondern am deutlich strengeren Computer-Grundrecht zu messen, dessen Anforderungen die Voraussetzungen des § 100 a StPO nicht genügen."

4. Anordnungsvoraussetzungen

a) § 11 Abs. 1a S. 1, 3 Nr. 1 lit. a) G10-E iVm. § 3 Abs. 1 G10

Für die Rechtfertigung setzen Eingriffe in das Fernmeldegeheimnis grundsätzlich hinreichend gewichtige Schutzgüter sowie ausreichend konkretisierte Eingriffsschwellen voraus.[30]

aa) Eingriffsschwelle

§ 3 Abs. 1 G10 sieht als Voraussetzung eines Eingriffs in das Fernmeldegeheimnis tatsächliche Anhaltspunkte einer künftigen oder in der Vergangenheit liegenden Straftatbegehung vor.[31]

Die hiermit für eine Beschränkung des Fernmeldegeheimnisses im Einzelfall vorgesehenen Anforderungen begegnen – unabhängig von der geplanten Neuregelung – grundsätzlichen verfassungsrechtlichen Bedenken:

Gerade im Vorfeldbereich ist die Gefahr von Fehlprognosen besonders hoch. Für entsprechend zu charakterisierende Befugnisse verlangt das Bundesverfassungsgericht deshalb handlungsbegrenzende Tatbestandselemente, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten sind.[32]

Einer von diesen Voraussetzungen abweichender, „geheimdienstspezifischer" Maßstab für die Eingriffstatbestände wäre nur dann zu rechtfertigen, wenn die Gefahr der Betroffenen, aufgrund falsch positiver Prognosen zum Adressaten von Folgemaßnahmen zur werden, bei Maßnahmen nach § 1 Nr. 1 iVm. § 3 G10 gegenüber Maßnahmen der Polizei oder Strafverfolgungsbehörden signifikant gesenkt wäre. Dies kann jedoch allenfalls insoweit angenommen werden, soweit – wie etwa bei der Auslandsaufklärung durch den BND – die Maßnahmen eindeutig zur Information der Bundesregierung für Tätigkeiten der Staatsleitung erhoben werden.[33] Soweit die Aufgabe des Verfassungsschutzes aber gerade und zunehmend in der vorbereitenden Gefahrenabwehr gesehen wird, bestehen keine Gründe, eine Absenkung der Anforderungen vorzunehmen.[34]

[30] B. Rusteberg, Die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz, KritV 2017, 24 (30).
[31] F. Roggan, G10, 2. Aufl. 2018, G 10 § 1 Rn. 12.
[32] F. Roggan, G10, 2. Aufl. 2018, G 10 § 3 Rn. 7, m.w.N.
[33] BVerfG, Urteil vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 1-332, Rn. 223 ff.; BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94 –, BVerfGE 100, 313-403, Rn. 283 ff.; vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350, Rn. 255; BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260-385, Rn. 232; insoweit übersieht Huber, in: Schenke/Graulich/Ruthig (Hrsg.), 2. Aufl. 2018, G 10 § 3 Rn. 9, dass sich die Ausführungen gerade auf die strategische Überwachung beziehen.
[34] F. Roggan, G10, 2. Aufl. 2018, G 10 § 3 Rn. 7, m.w.N.

bb) Rechtsgüter

Der Regelungsansatz des § 3 Abs. 1 G10 kann schon deshalb nicht überzeugen, weil dieser als Voraussetzung präventiver Befugnisse nicht auf die maßgeblichen Rechtsgüter, sondern ausschließlich auf die Verhinderung bestimmter Straftaten abgestellt wird.[35]

Auch die im Einzelnen vorgesehenen Anlassdelikte stehen zu Recht in der Kritik: Bei vielen von ihnen handelt es sich wiederum um Gefährdungsdelikte, die mithin keine konkrete Rechtsgutsverletzung und teilweise noch nicht einmal eine konkrete Gefährdung voraussetzen. In Verbindung mit der (unzureichenden) Eingriffsschwelle findet insofern eine sich gegenseitig potenzierende Vorverlagerung des Eingriffspunktes statt.[36]

Schließlich finden sich verschiedene Delikte im Katalog, die mit einer Höchststrafe von drei Jahren (vgl. § 130 Abs. 4 StGB) oder auch nur einem Jahr (vgl. etwa § 20 Abs. 1 VereinsG) bedroht sind. Wenn im Regelungsansatz gerade nicht auf die gefährdeten Rechtsgüter, sondern auf einzelne Delikte abgestellt wird, kann hier kaum von einem hinreichenden Gewicht dieser Straftaten für die Eingriffsrechtfertigung ausgegangen werden.[37]

b) § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E iVm. § 3 G10

Da § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme darstellt, unterliegt die Regelung strengen Anforderungen: Sie müsste insoweit gesetzlich voraussetzen, dass tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen.

Derartige Anforderungen finden sich in dem auch an dieser Stelle insoweit maßgeblichen § 3 G10 gerade nicht. § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E ist somit offensichtlich verfassungswidrig.

5. Verfahrensanforderungen und Umsetzbarkeit

Indem § 11 Abs. 1a S. 3 G10-E verlangt, dass technisch sicherzustellen sei, dass ausschließlich die laufende Kommunikation überwacht und aufgezeichnet werden kann, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und dass die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden müssen, greift die Regelung zum Teil wortwörtlich Formulierungen des Bundesverfassungsgerichts auf. Damit kann zwar sichergestellt werden, dass die Regelung insoweit unter die Schutzbereichsausnahme des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme fällt.

[35] Vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 105 f.: „Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es auf das Gewicht der verfolgten Straftaten an […]. Für Maßnahmen, die der Gefahrenabwehr dienen und damit präventiven Charakter haben, kommt es unmittelbar auf das Gewicht der zu schützenden Rechtsgüter an."

[36] F. Roggan, G10, 2. Aufl. 2018, G 10 § 3 Rn. 10, m.w.N.

[37] F. Roggan, G10, 2. Aufl. 2018, G 10 § 3 Rn. 10, m.w.N.

Es bleibt aber – wie schon bei der Neuregelung des § 100a StPO[38] – weiterhin vollkommen offen, wie eine solche Sicherstellung technisch erreicht werden kann. Auch die Entwurfsbegründung schweigt sich offensiv hinsichtlich dieses Punktes aus.

Mehr als fünf Jahre nach der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz machen es Bestimmtheitsgrundsatz und Wesentlichkeitsgebot aber notwendig – ggf. im Wege der delegierten Normsetzung durch Verordnung –, mindestens im Grundsatz festzulegen, welche technischen Anforderungen zu treffen sind, um diese Punkte tatsächlich sicherzustellen.[39]

Auch verfahrensmäßige Sicherungen – etwa durch eine Vorabkontrolle der Software – sind insoweit nicht vorgesehen.[40] Eine nachträgliche Kontrolle wird hingegen dadurch nahezu verunmöglicht, dass momentan auch keinerlei erprobte technische Verfahren bekannt, die nachweisen könnten, was für eine Software auf einem kontrolliertem System zu einem bestimmten Zeitpunkt lief und was diese dort bewirkt hat.[41]

Eine Begrenz- und Kontrollierbarkeit des tatsächlich erfolgenden Einsatzes der Überwachungssoftware ist – soweit ersichtlich – momentan weder rechtlich- noch technisch erreichbar.

6. Verhältnismäßigkeit im Übrigen

Offen bleibt nach der Gesetzesbegründung auch, inwieweit tatsächlich ein Bedürfnis für eine derartige Quellen-TKÜ besteht. Dabei ist zwar die Erforderlichkeit der Maßnahme nach § 11 Abs. 1a G10-E insoweit sichergestellt, als diese nur eingesetzt werden darf, „wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen“. Ein Einsatz der Quellen-TKÜ scheidet demnach also von vornherein in allen Situationen aus, in denen eine Überwachung auf anderem Wege möglich ist.

Tatsächlich bestehen mittlerweile aber auch bei verschlüsselten Datentransfers durchaus Alternativen zum Einsatz der Quellen-TKÜ.[42] Überdies ist kommt die Technik bislang auch dort, wo gesetzliche Ermächtigungen für ihren Einsatz bestehen, nur äußerst sporadisch zum Einsatz gekommen: So haben Polizei und Ermittlungsbehörden nach der Justizstatistik des Jahres 2019 die Online-Durchsuchung nach der StPO in 21 Verfahren 33 Mal angeordnet und in 12 Fällen tatsächlich eingesetzt. Die Quellen-TKÜ wurde bei 31 Anordnungen sogar lediglich in drei Fällen tatsächlich eingesetzt.[43]

---

[38] Siehe D. Brodowski/U. Sieber, in: Hoeren/Sieber/Holznagel MMR-HdB, 54. EL Oktober 2020, Teil 19.3 Strafprozessrecht, Rn.150.

[39] M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra, 24/20, 1 (8), auch zu möglichen technischen Ansätzen.

[40] M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra, 24/20, 1 (10 f.).

[41] F. Freiling/C. Safferling/C. Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung, JR 2018, 9 (20).

[42] Vgl. etwa die diesbezüglichen Ausführungen M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra 24/2020, 1 (12 ff.).
etwa https://netzpolitik.org/2021/ohne-staatstrojaner-polizei-und-geheimdienste-koennen-whatsapp-mitlesen/.

[43] https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/.

Angesichts der erheblichen Nachteile, die das Vorhalten einer entsprechenden Technik bereits strukturell für die Freiheitsrechte mit sich bringt – Vertrauenseinbußen, Sicherheitslücken[44], Missbrauchsgefahr – werfen diese Punkte weitere dringende Fragen bezüglich der Angemessenheit der Regelungen auf, die die Gesetzesbegründung bislang nicht einmal ansatzweise adressiert.

II. Nummer 7 lit. a) - § 11 Abs. 1b G10-E

7. § 11 wird wie folgt geändert:

a) Nach Absatz 1 werden die folgenden Absätze 1a und 1b eingefügt: […]

(1b) Werden nach der Anordnung weitere Kennungen von Telekommunikationsanschlüssen der Person, gegen die sich die Anordnung richtet, bekannt, darf die Durchführung der Beschränkungsmaßnahme auch auf diese Kennungen erstreckt werden. Satz 1 findet keine Anwendung auf weitere Kennungen von Telekommunikationsanschlüssen von Personen, gegen die sich die Anordnung richtet, weil auf Grund bestimmter Tatsachen anzunehmen ist, dass der Verdächtige ihren Anschluss benutzt (§ 3 Absatz 2 Satz 2 Variante 3). Bevor die Durchführung der Beschränkungsmaßnahme nach Satz 1 auf eine weitere Kennung erstreckt wird, ist dies der nach § 10 Absatz 1 zur Anordnung zuständigen Behörde anzuzeigen. Das nach § 10 Absatz 1 zuständige Bundesministerium unterrichtet monatlich die G 10-Kommission über die ihm nach Satz 3 angezeigten Erstreckungen.“

Nach § 11 Abs. 1b G10-E darf die Durchführung der Beschränkungsmaßnahme auf Kennungen von Telekommunikationsanschlüssen der Person, gegen die sich die Anordnung richtet, erstreckt werden, soweit diese Kennungen nach der Anordnung bekannt werden.

Durch diese Regelung werden zunächst die Verfahrensregelungen der §§ 9 f. G10 ausgehebelt, die Beschränkungsmaßnahmen von einer auf einen vorherigen Antrag erteilten Anordnung durch die zuständigen Landesministerium bzw. das Bundesinnenministerium abhängig machen. Zugleich wird damit das Erfordernis beseitigt, den Vollzug der Maßnahme bis zur Zustimmung der G10-Kommission aufzuschieben, da sich diese nach § 15 Abs. 6 G10-E nur auf die vom Bundesministerium angeordneten Beschränkungsmaßnahmen bezieht. In den Fällen des § 11 Abs. 1b G10-E wird das Bundesministerium aber gerade nur über die Erweiterung der Beschränkungsmaßnahmen informiert, ordnet diese aber nicht selbst an.

Angesichts der weiten Auslegung des Begriffs der Telekommunikation[45] ist dabei kaum abzuschätzen, was als „Kennung von Telekommunikationsanschlüssen“ in den Anwendungsbereich des § 11 Abs. 1b G10-E fällt. Betroffen können keineswegs nur „klassische“ Telefonnummern, Email-Adressen oder Messengerprofile sein, sondern letztlich sämtliche Kennungen, die im Internetverkehr eine Zuordnung zu einer Adresse ermöglichen. Letztlich wird hier eine Rundumüberwachung ohne nennenswerte verfahrensrechtliche Sicherungen ermöglicht.

[44] Dazu ausf. 19(4)844 A - Stellungnahme Prof. Dr. Matthias Bäcker, S. 7 ff.
[45] Siehe oben I.3.a).

Die Regelung des § 11 Abs. 1b G10-E ist deshalb als unangemessen und unverhältnismäßig zu charakterisieren.

Soweit es der Regelung gerade um die Vermeidung von Verzögerungen im Vollzug geht, kann dabei ohne Weiteres auf die neu geschaffene Eilanordnung nach § 15a G10-E zurückgegriffen werden. Bei dieser sind zumindest die Nachvollziehbarkeit des Verfahrens und eine zeitige Interventionsmöglichkeit der G10-Kommission sichergestellt.

Freilich ist auch an dieser Stelle zu fragen, inwieweit eine nachrichtendienstliche Voraufklärung überhaupt ein geeignetes Vorgehen in Eilfällen darstellt.

III. Nummer 5 - § 2 Abs. 1a u. 1b G10-E

Die Regelung des § 2 Abs. 1a u. 1b G10-E geht mit weitreichenden Eingriffen in die Rechte der Anbieter von Telekommunikationsdienstleistern einher. Diese haben der jeweiligen Behörde u.a. nach § 2 Abs. 1a S. 1 Nr. 4 G10-E die Einbringung von technischen Mitteln zur Durchführung einer Maßnahme nach § 11 Absatz 1a durch Unterstützung bei der Umleitung von Telekommunikation durch die berechtigte Stelle zu ermöglichen, Zugang zu ihren Einrichtungen während der üblichen Geschäftszeiten zu gewähren sowie die Aufstellung und den Betrieb von Geräten für die Durchführung der Maßnahme zu ermöglichen.

Anfallende Datenströme sollen danach nicht mehr nur einfach kopiert, sondern umgeleitet werden. Damit können die betroffenen Datenströme verändert werden, d.h. es können sowohl übermittelte Daten inhaltlich verändert, als auch Daten hinzugefügt oder unterdrückt werden.[46]

Der Eingriff in die Berufsfreiheit der Unternehmen, der durch entsprechende Pflichten – gleich ob aktiv oder zur Duldung – sowie die mit diesen verbundenen finanziellen Belastungen bewirkt wird, ist nach der Rechtsprechung des 2. Senats des Bundesverfassungsgerichts als grundsätzlich gerechtfertigt anzusehen.[47]

Dessen ungeachtet ist nicht nachvollziehbar, weshalb der Gesetzentwurf auf konkretisierende Regelungen, insbesondere in Hinblick auf die zahlreichen entstehenden Haftungsfragen vollständig verzichtet. So weist der Branchenverband „bitkom“ in seiner Stellungnahme etwa zutreffend darauf hin, dass im Gesetzentwurf offengelassen werde, was in Fällen passiere, in denen die an den informationstechnischen Systemen vorgenommenen Änderungen nicht gem. § 11 Abs. 1a S. 3 Nr. 3 G10-E rückgängig gemacht werden können.[48]

46 eco, Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Berlin, 30.06.2020, S. 5.
47 BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018 – 2 BvR 2377/16 –, juris.
48 bitkom, Stellungnahme Anpassung des Verfassungsschutzrechts, 30.06.2020 S. 3.

Darüber hinaus hat sich das Bundesverfassungsgericht in der oben genannten Rechtsprechung ausdrücklich nicht hinsichtlich der datenschutzrechtlichen Konsequenzen etwaiger Verpflichtungen der Telekommunikationsanbieter geäußert.[49]

Diesbezüglich weisen die Diensteanbieter auch über ihren Branchenverband auf die mit entsprechenden Maßnahmen verbundenen hohen Risiken für die gesamte Netzintegrität hin, die dadurch entstehen, dass die Anbieter ihnen nicht näher bekannte Schadsoftware über ihre Netze in das entsprechende Computersystem einschleusen müssen. Überdies seien solche Maßnahmen jedenfalls geeignet, das Vertrauen in die Kommunikation einschließlich aller abgerufenen Informationen massiv und dauerhaft zu untergraben.[50]

Ergänzend ist auf das extreme Missbrauchspotential hinzuweisen, das die Eröffnung derart weitreichender und letztlich nicht kontrollierbarer Zugriffsmöglichkeiten durch die Nachrichtendienste mit sich bringt. Ohne dass dies von dritter Seite technisch in irgendeiner Weise nachvollziehbar ist, können die Nachrichtendienste faktisch nahezu beliebig gesendete Daten manipulieren und sich auf diesem Wege Zugriffsmöglichkeiten auf informationstechnische Systeme verschaffen. Inwiefern in informationstechnischen Systemen gespeicherten Daten damit zukünftig überhaupt noch ein Beweiswert zugeordnet werden kann, bleibt offen.

Demgegenüber zielt das Recht auf informationelle Selbstbestimmung gerade auch darauf ab, im Sinne eines vorgelagerten Grundrechtsschutzes derartige Missbrauchsgefahren zu verhindern.[51] Mit Blick auf die objektive Dimension des Rechts auf informationelle Selbstbestimmung ist deshalb bereits die Eröffnung derartiger Zugriffsmöglichkeiten für die Nachrichtendienste als unverhältnismäßig anzusehen.

D. Fazit

Der vorliegende Gesetzesentwurf vertieft die Rolle des Verfassungsschutzes als besondere Gefahrenabwehrbehörde. Damit werden jedoch nicht nur das Trennungsgebot und eine sich daraus ergebende mögliche Eingriffsprivilegierung der Verfassungsschutzbehörden zusätzlich in Frage gestellt, sondern – angesichts der Kompetenzüberschneidungen mit der Polizei – auch die Existenz der Verfassungsschutzbehörden selbst.

- Auch vor diesem Hintergrund ist die Erweiterung des Einbezugs der Beobachtung von Einzelpersonen durch das BfV nach § 4 Abs. 1 BVerfSchG-E abzulehnen. Sie ist, gerade angesichts der in der Entwurfsbegründung genannten Beispiele, schon nicht erforderlich.
- Die Regelung des § 11 Abs. 1a S. 1, 3 Nr. 1 a) G10-E partizipiert an den bekannten Mängeln des Anforderungskatalogs in § 3 Abs. 1 G10 und leidet an fehlenden verfahrensrechtlichen

49 BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018 – 2 BvR 2377/16 –, juris, Rn. 51.
50 eco, Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Berlin, 30.06.2020, S. 2 f.
51 Dazu R. Poscher, Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Gander/Perron/ders./Riescher/Würtenberger (Hrsg.), Resilienz in der offenen Gesellschaft, 2012, S. 167 ff.; G. Britz, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 ff.

Regelungen, wie eine Begrenzung der Überwachung technisch und rechtlich sichergestellt werden kann.

- Die Regelung des § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E greift in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein, ohne an die damit korrespondierenden Voraussetzungen gebunden zu werden, und ist damit offensichtlich verfassungswidrig.
- § 11 Abs. 1b G10-E ermöglicht eine Rundumüberwachung ohne verfahrensrechtliche Kontrolle und ist deshalb unverhältnismäßig.
- Angesichts des sich aus der Regelung ergebenden erheblichen Missbrauchspotentials verstößt § 2 Abs. 1a u. 1b G10-E gegen die objektive Dimension des Rechts auf informationelle Selbstbestimmung.