RA Dr. Bijan Moini • [redacted]

An das
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

Rechtsanwalt Dr. Bijan Moini M.A.

[redacted]

E-Mail: [redacted]
Tel.: [redacted]
Fax: [redacted]

7. Juli 2022

Verfassungsbeschwerde

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]
7. [redacted]
8. [redacted]
9. [redacted]
10. [redacted]

– Beschwerdeführer*innen –

Bevollmächtigter: Rechtsanwalt Dr. Bijan Moini, [redacted]

gegen

§ 6 Abs. 1 i.V.m. Abs. 2 Satz 1,

§ 6 Abs. 2 Satz 2

und

§ 6 Abs. 2 Satz 4 i.V.m. § 10 Abs. 1

des Bundesverfassungsschutzgesetzes (BVerfSchG) in der Fassung vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Artikel 1 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274),

§ 11 Abs. 1a Satz 1 i.V.m. § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1,

§ 11 Abs. 1a Satz 1 i.V.m. § 3 Abs. 1 Satz 2,

§ 11 Abs. 1a Satz 2 i.V.m. § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1,

§ 11 Abs. 1a Satz 2 i.V.m. § 3 Abs. 1 Satz 2,

§ 3 Abs. 2 Satz 2,

§ 3a,

§ 11 Abs. 1b Satz 1,

§ 12 Abs. 1 Satz 2 bis 5,

§ 13,

§ 15a,

und

§ 4 Abs. 4 Satz 1 und 2,

des Artikel 10-Gesetzes (G 10) in der Fassung vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2017 I S. 154), zuletzt geändert durch Artikel 6 Absatz 4 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274) und

§ 3 Abs. 3 Satz 1-2,

und

§ 3 Abs. 3 Satz 3 (i.V.m. § 6 Abs. 1 Satz 4 i.V.m. § 10 Abs. 1 BVerfSchG)

des Gesetzes über den militärischen Abschirmdienst (MADG) in der Fassung vom 20. Dezember 1990 (BGBl. I S. 2954, 2977), zuletzt geändert durch Artikel 2 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274).

Namens und in Vollmacht der Beschwerdeführer*innen (**Anlage**) erhebe ich Verfassungsbeschwerde und rüge die Verletzung von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1 und Art. 19 Abs. 4 GG.

Gliederung des Schriftsatzes

A. Vorbemerkungen

Die Landesparlamente und der Deutsche Bundestag haben in den vergangenen Jahren die Sicherheitsbehörden mit umfassenden neuen Befugnissen ausgestattet. Zwei Arten von Befugnissen standen ganz besonders im Fokus auch des angerufenen Gerichts: die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung. Mit diesen beiden Instrumenten möchten die Sicherheitsbehörden die Herausforderungen bewältigen, vor die sie die Digitalisierung stellt. Während die Quellen-Telekommunikationsüberwachung auf den Schutz elektronischer Kommunikation durch Verschlüsselungstechniken reagiert, öffnet die Online-Durchsuchung die Tür zum digitalen Archiv unseres Lebens.

Beides genießt unter dem Grundgesetz einen herausragenden Schutz. Art. 10 Abs. 1 GG schützt die vertrauliche Kommunikation. Das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG schützt eben diese Systeme. Letzteres Grundrecht hat das angerufene Gericht gerade zum Schutz vor ungerechtfertigten Online-Durchsuchungen entwickelt.

Die vorliegende Verfassungsbeschwerde richtet sich im Schwerpunkt gegen eine neue Befugnisnorm im Artikel 10-Gesetz, die es insgesamt 19 deutschen Nachrichtendiensten erlaubt, unter bestimmten Voraussetzungen IT-Systeme zu infiltrieren sowie die laufende (Quellen-Telekommunikationsüberwachung) und gespeicherte oder „ruhende“ (aufgrund dieser Einschränkung „beschränkte“ Online-Durchsuchung) Telekommunikation auszuspähen. Unter die „Telekommunikation“ fällt ein breites Spektrum an sehr persönlichen Daten. Dazu zählen unter anderem Telefonate, Sprachnachrichten, Chat-Nachrichten und SMS, in sozialen Netzwerken geteilte Inhalte, Kommentare, mit anderen Personen geteilte Daten, das Surfverhalten, hoch- oder heruntergeladene Dateien auch aus Clouds etc.

Das angerufene Gericht hat sich mit der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung bereits in verschiedenen Verfahren beschäftigt (insbesondere BVerfGE 120, 274; BVerfGE 141, 220). Jüngst hat sich das angerufene Gericht zudem grundsätzlich mit den Voraussetzungen nachrichtendienstlicher Überwachungsbefugnisse auseinandergesetzt und deren Grundlagen und Voraussetzungen näher beschrieben (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17). Mit dem vorliegenden Verfahren erhält das Gericht Gelegenheit dazu, diese Maßstäbe auf die zwei hier angegriffenen, besonders eingriffsintensiven Instrumente und ihren Einsatz durch die Nachrichtendienste anzuwenden. Zugleich kann sich das Gericht mit einigen grundsätzlichen Problemen auseinandersetzen, die das Artikel 10-Gesetz schon lange aufwirft. Dazu zählen die Eingriffsschwellen, Schutzzwecke, Verfahrenssicherungen und Übermittlungsbefugnisse. Es wird aufgezeigt, dass die angegriffenen Rechtsnormen die in den genannten Entscheidungen formulierten Anforderungen nicht erfüllen und verfassungswidrig sind.

Die angegriffenen Befugnisnormen haben auch in einer weiteren Dimension eine erhebliche Tragweite. So wird durch sie der Anreiz geschaffen, Sicherheitslücken informationstechnischer Systeme geheim zu halten. Diese Sicherheitslücken werden aber nicht nur von staatlichen Stellen in Deutschland genutzt. Vielmehr können auch Dritte diese für ihre Zwecke ausnutzen, was die Allgemeinheit, mehr aber noch besonders schutzbedürftige Personen, großen Gefahren aussetzt. Den Staat trifft eine Schutzpflicht zur Abwehr derartiger Gefahren. Indem Anreize zur Verheimlichung der Schutzlücken gesetzt werden, ohne zugleich die Voraussetzungen zur Offenbarung derartiger Lücken zu regeln, wird diese Schutzpflicht ignoriert und damit verletzt.

Die Verfassungsbeschwerde wirft außerdem die Frage auf, unter welchen Voraussetzungen die Nachrichtendienste Informationen untereinander austauschen dürfen. Anlass dafür bietet die Einbindung des Militärischen Abschirmdienstes (MAD) in das nachrichtendienstliche Informationssystem. Auch diese Frage hat das angerufene Gericht bislang nicht geklärt. Entscheidungen zu verwandten Konstellationen (insbesondere BVerfGE 125, 260; 130, 151; 133,

277; 156, 11) lassen sich Maßstäbe auch für ein derartiges Informationssystem entnehmen. Die angegriffenen Normen verletzen auch diese Maßstäbe und sind ebenfalls verfassungswidrig.

B. Gegenstand der Verfassungsbeschwerde

Gegenstand der Verfassungsbeschwerde sind die Neuregelungen des Artikel 10-Gesetzes, des Bundesverfassungsschutzgesetzes und des Gesetzes über den militärischen Abschirmdienst durch das Gesetz zur Anpassung des Verfassungsschutzrechts, in Kraft getreten am 9. Juli 2021 (BGBl. I S.2274).

Ausweislich der Gesetzesbegründung soll das Gesetz aktuellen Herausforderungen insbesondere im Bereich des internationalen Terrorismus und des Rechtsterrorismus zugunsten der Aufklärung schwerer Bedrohungen für den demokratischen Rechtsstaat und die freiheitliche demokratische Grundordnung Rechnung tragen. Hierzu sieht das Gesetz unter anderem eine Ergänzung der Regelungen zur Telekommunikationsüberwachung vor. Zudem ermöglicht das Gesetz dem MAD, am nachrichtendienstlichen Informationssystem teilzunehmen.

BT-Drs. 19/24785, S. 1.

Gegenstand der Verfassungsbeschwerde sind die entsprechenden Befugnisnormen. Des Weiteren richtet sich die Verfassungsbeschwerde gegen die Untätigkeit des Gesetzgebers, den staatlichen Umgang mit zur Kenntnis gelangten Sicherheitslücken zu regeln. Darüber hinaus sind die mit den Ermächtigungsnormen im Zusammenhang stehenden Vorschriften zum Verfahren und zur Informationsübermittlung Gegenstand dieser Verfassungsbeschwerde.

I. Angegriffene Regelungen im Einzelnen

Erstens richtet sich die Verfassungsbeschwerde gegen die Ermächtigung zur Überwachung der *laufenden* Telekommunikation unter Eingriff in ein informationstechnisches System (§ 11 Abs. 1a Satz 1 i.V.m. § 3 Abs. 1 G 10) sowie die mit dieser Ermächtigung im engen Zusammenhang stehenden unzureichenden Verfahrensregelungen und Schutzvorkehrungen, namentlich

> die Vorschrift über das Vorgehen gegen nicht verantwortliche Personen (§ 3 Abs. 2 Satz 2 G 10),
>
> den Ausnahmetatbestand zum Schutz des Kernbereichs privater Lebensgestaltung im Einzelfall (§ 3a G 10),
>
> die gegenüber den Tatbestandsvoraussetzungen des § 11 Abs. 1a G 10 vereinfachte Erstreckung der Überwachung auf weitere Kennungen (§ 11 Abs. 1b Satz 1 G 10),
>
> die Vorschrift über zu unterbleibende Mitteilungen an Betroffene (§ 12 Abs. 1 Satz 2 bis 5 G 10),
>
> die Beschränkung des Rechtswegs vor erteilter Mitteilung an den Betroffenen (§ 13 G 10),
>
> die selbständige Anordnung der Überwachungsmaßnahme im Eilfall ohne Zustimmung der G 10-Kommission (§ 15a G 10).

Zweitens richtet sich die Verfassungsbeschwerde gegen die Ermächtigung zur Überwachung der *ruhenden* Telekommunikation unter Zugriff auf ein informationstechnisches System (§ 11 Abs. 1a Satz 2 i.V.m. § 3 Abs. 1 G 10) sowie in diesem Zusammenhang ebenfalls gegen die bereits zuvor genannten verfahrensrechtlichen Vorschriften.

Drittens wird das Unterlassen der spezifischen Regelung eines Schwachstellenmanagements von Sicherheitslücken informationstechnischer Systeme gerügt, welche als Ausgleich zu den obigen Eingriffsbefugnissen den Zielkon-

flikt zwischen Geheimhaltungsinteressen der Nachrichtendienste und der Gefahren durch offenbleibende Sicherheitslücken auflöst.

Viertens wird die Reichweite der Befugnis zur Übermittlung von Informationen an andere Stellen im In- und Ausland (§ 4 Abs. 4 Satz 1 und Satz 2 G 10) angegriffen.

Fünftens richtet sich die Verfassungsbeschwerde gegen die Erweiterung des nachrichtendienstlichen Informationssystems, konkret gegen

> die Übermittlungspflichten zwischen den Landesbehörden für Verfassungsschutz und dem Bundesamt für Verfassungsschutz (§ 6 Abs. 1 BVerfSchG),
>
> die in Erfüllung der vorgenannten Übermittlungspflichten eröffnete Möglichkeit, den MAD in den Informationsverbund der Verfassungsschutzbehörden zu integrieren (§ 6 Abs. 2 BVerfSchG),
>
> die kongruenten Übermittlungspflichten des MAD gegenüber den Verfassungsschutzbehörden sowie die zu § 6 Abs. 2 BVerfSchG komplementäre Rechtsgrundlage zur Teilnahme am nachrichtendienstlichen Informationsverbund (§ 3 Abs. 3 MADG).

II. Erläuterung der angegriffenen Vorschriften

§ 11 Abs. 1a Satz 1 G 10 ermächtigt die Behörden eine Quellen-Telekommunikationsüberwachung zur Überwachung von verschlüsselter laufender Kommunikation durchzuführen. Heutzutage nutzen viele Kommunikationsprogramme standardmäßig eine Verschlüsselung der Daten, die ohne aktives Handeln der Nutzer*innen im Hintergrund arbeitet. Zur Umgehung dieser Schutzvorkehrungen erfasst diese besondere Form der Telekommunikationsüberwachung die Kommunikation bereits „an der Quelle", somit entweder bevor die Daten verschlüsselt oder nachdem diese entschlüsselt wurden. Dementsprechend ermöglicht § 11 Abs. 1a Satz 1 G 10 den Einsatz der Quellen-Telekommunikationsüberwachung insbesondere zur Überwachung und Aufzeichnung von Kommunikation in unverschlüsselter Form zu ermöglichen. Dazu bedarf es der Infiltration des informationstechnischen Systems mit einer speziellen Software, welche die verdeckte Überwachung möglich macht – dem sogenannten Staatstrojaner.

Dabei unterliegt § 11 Abs. 1a Satz 1 G 10 denselben Voraussetzungen, wie auch andere Formen der Telekommunikationsüberwachung. Konkret sind die Voraussetzungen in § 3 G 10 geregelt. § 3 Abs. 1 Satz 1 G 10 ermöglicht den Einsatz der Quellen-Telekommunikationsüberwachung, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass eine in der Vorschrift aufgeführte Anlasstat geplant oder begangen wird oder schon begangen wurde. § 3 Abs. 1 Satz 2 G 10 ermöglicht außerdem den Einsatz, wenn tatsächliche Anhaltspunkte dafür bestehen, dass jemand Mitglied in einer Vereinigung ist, deren Zwecke oder 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.

§ 11 Abs. 1a Satz 2 G 10 bildet die Ermächtigungsnorm für beschränkte Online-Durchsuchung. Bei beiden Überwachungsmaßnahmen infiltrieren Behörden informationstechnische Systeme, allerdings mit unterschiedlichen Zielrichtungen: Während bei der Quellen-Telekommunikationsüberwachung eine

laufende Kommunikation überwacht werden soll, die aufgrund ihrer Verschlüsselung anderweitig nicht ausgewertet werden kann, wird mit der beschränkten Online-Durchsuchung besonders der Zugriff auf den Speicher des Zielsystems bezweckt, um nach bestimmten Dateien zu suchen.

Vgl. *Bär*, in: BeckOK PolR Bayern, 18. Aufl. 2022, PAG, Art. 42 Rn. 41.

Die für die Durchführung der Überwachungsbefugnisse notwendige Infiltration der Zielsysteme erfolgt in der Regel, indem die Nachrichtendienste durch die Ausnutzung in informationstechnischen Systemen ausnutzen.

§ 2 Abs. 6 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) definiert Sicherheitslücken als „Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können."

Innerhalb dieser Definition werden Sicherheitslücken (synonym: Schwachstellen) danach unterschieden, ob sie Hersteller*innen bereits bekannt – dann n-Days, im Sinne von: Hersteller*innen bereits seit n Tagen bekannt – oder noch unbekannt sind – dann Zero-Days, Hersteller*innen null Tage bekannt. Aus der Perspektive der Sicherheit von informationstechnischen Systemen, die mit der fehlerhaften Software arbeiten, unterscheiden sich n-Days und Zero-Days fundamental:

Für Zero-Days stehen noch keine technischen Lösungen – sogenannte Fixes oder Patches – bereit. Eine Ausnahme besteht nur in dem seltenen Fall, dass Hersteller*innen die Software auch in Unkenntnis der Sicherheitslücke durch Zufall so ändern, dass die Lücke gleichsam „nebenbei" geschlossen wird.

Für n-Days hingegen besteht für die Hersteller*innen des betroffenen Systems die Möglichkeit, Gegenmittel zu entwickeln.

Zero-Day-Schwachstellen bergen folglich eine höhere Gefahr. Gerade der Mangel an technischen Lösungen für diese gefährlichen Schwachstellen veran-

lasst jedoch die Nachrichtendienste, diese zu suchen. Dieser ermöglicht insbesondere eine längerfristige Ausnutzung der Schwachstellen für die bezweckten nachrichtendienstlichen Überwachungsmaßnahmen. Die Gefährlichkeit von Zero-Day-Schwachstellen intensiviert sich zusätzlich, wenn für anfällige Systeme ein funktionierender Angriffscode bereits in bekannte Angriffswerkzeuge integriert wurde. Dies macht eine breitere Ausnutzung – und somit auch einen Missbrauch durch kriminelle Dritte – höchstwahrscheinlich. Das gilt insbesondere für den – gesetzlich nicht ausgeschlossenen und in der Praxis relevanten – Fall, dass die Behörden Angriffswerkzeuge nutzen, die von privaten Unternehmen entwickelt wurden und auch Dritten angeboten werden.

Das Informationssystem der Nachrichtendienste beinhaltet einen umfassenden gemeinsamen Datenverbund der Verfassungsschutzbehörden, das Nachrichtendienstliche Informationssystem und Wissensnetz (NADIS-WN). Darin werden personenbezogene Daten jeglicher Art und Herkunft in einer zentralen, automatisiert auswertbaren Verbunddatei gespeichert (§ 6 Abs. 2 Satz 1 BVerfSchG). Darüber hinaus eröffnen nunmehr § 6 Abs. 2 Satz 2 BVerfSchG und § 3 Abs. 3 Satz 2 MADG die Möglichkeit, den MAD in das nachrichtendienstliche Informationssystem einzubinden.

III. Die Beschwerdeführer*innen

Alle Beschwerdeführer*innen nutzen privat wie beruflich, teilweise auch im Rahmen ihres politischen Engagements, informationstechnische Systeme wie PCs und Laptops, verfügen über einen Internetzugang und haben ein internetfähiges Mobiltelefon. Sie nutzen zudem Girokonten und weitere Finanzdienstleistungen, sowohl privat als teilweise auch in ihrer Eigenschaft als Funktionär*innen politischer Organisationen. Zudem verreisen sämtliche Beschwerdeführer*innen gelegentlich mit dem Flugzeug.

1. Beschwerdeführerin zu 1

[redacted]

[redacted]

2. Beschwerdeführerin zu 2

[redacted]

[redacted]

3. Beschwerdeführer zu 3

[redacted]

[redacted]

4. Beschwerdeführer zu 4

[redacted]

[redacted]

5. Beschwerdeführer zu 5

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6. Beschwerdeführer zu 6

[redacted]

[redacted]

7. Beschwerdeführer zu 7

[redacted]

[redacted]

8. Beschwerdeführerin zu 8

[redacted]

9. Beschwerdeführerin zu 9

[redacted]

10. Beschwerdeführer zu 10

[redacted]

C. Zulässigkeit

I. Statthafter Beschwerdegegenstand

Die angegriffenen Regelungen sind statthafte Beschwerdegegenstände.

Bei den neu geschaffenen Normen handelt es sich um Akte öffentlicher Gewalt im Sinne von Art. 93 Abs. 1 Nr. 4a GG, § 90 Abs. 1 BVerfGG. Die Normen sind vom Deutschen Bundestag erlassene Gesetze und somit Akte der Legislative.

Die angegriffenen Regelungen sind auch insofern zulässige Beschwerdegegenstände, als die Verletzung objektiver Schutzpflichten aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG durch Unterlassen von Begleitregelung zum behördlichen Umgang mit informationstechnischen Sicherheitslücken gerügt wird.

> Vgl. BVerfGE 158, 170 <182 f. Rn. 22>.

II. Beschwerdebefugnis

Die Beschwerdeführer*innen sind im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt. Sie sind selbst, gegenwärtig und unmittelbar von den Regelungen betroffen.

1. Telekommunikationsüberwachung (Beschwerdeführer*innen zu 1 bis 5 und 7)

a) Verfassungsrechtliche Rügen

Die Beschwerdeführer*innen zu 1 bis 5 und 7 machen geltend, durch die angegriffenen Überwachungsbefugnisse in § 11 Abs. 1a i.V.m. § 3 Abs. 1 G 10 in ihrem Recht auf Achtung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG und ihrem Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt zu sein.

Zudem machen die Beschwerdeführer*innen zu 1 bis 5 und 7 geltend, aufgrund mangelhafter Rechtsschutzsicherungen im Zusammenhang mit den genannten Befugnissen in ihrem Recht auf effektiven Rechtsschutz aus Art. 19 Abs. 4 GG verletzt zu sein.

b) Eigene, gegenwärtige, unmittelbare Betroffenheit

(1) Eigene und gegenwärtige Betroffenheit

Die Beschwerdeführer*innen zu 1 bis 5 und 7 sind durch die Ermächtigungen des § 11 Abs. 1a i.V.m. § 3 Abs. 1 G 10 selbst und gegenwärtig betroffen.

Dies ist nach der Rechtsprechung des angerufenen Gerichts im Zusammenhang mit Ermächtigungsnormen zu verdeckten Überwachungsmaßnahmen

bereits dann der Fall, wenn mit einiger Wahrscheinlichkeit zukünftig eine Betroffenheit von derartigen Maßnahmen zu erwarten ist.

> Vgl. BVerfGE 100, 313 <354>; 109, 279 <307 f.>; 113, 348 <363>; 133, 277 <312 f.>; 141, 220 <262>; 143, 1 <21>; 155, 119 <160>; zuletzt BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 97 stRspr.

Ein Vortrag, für sicherheitsgefährdende oder nachrichtendienstlich relevante Aktivitäten verantwortlich zu sein, ist zum Beleg der Selbstbetroffenheit grundsätzlich nicht erforderlich.

> Vgl. BVerfGE 130, 151 <176 f.>; zuletzt BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 97 stRspr.

Die Beschwerdeführer*innen zu 1 bis 5 und 7 sind mit einer deutlich höheren Wahrscheinlichkeit als die allgemeine Bevölkerung Zielpersonen oder mitbetroffene Dritte der Telekommunikationsüberwachung.

(a) Beschwerdeführerinnen zu 1 und 2

[redacted]

[redacted]

[redacted]

(b) Beschwerdeführer zu 3, 4 und 7

[redacted]

[redacted]

(c) Beschwerdeführer zu 5

[redacted]

(2) Unmittelbare Betroffenheit

Die Beschwerdeführer*innen zu 1 bis 5 und 7 sind durch die angegriffenen Vorschriften auch unmittelbar betroffen.

Zwar bedürfen Ermächtigungen zu Überwachungsmaßnahmen wie § 11 Abs. 1a G 10 der behördlichen Umsetzung. Von einer unmittelbaren Betroffenheit durch ein Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführer*innen den Rechtsweg nicht beschreiten können, weil sie keine Kennt-

nis von der betreffenden Vollziehungsmaßnahme erhalten. In solchen Fällen steht ihnen die Verfassungsbeschwerde unmittelbar gegen das Gesetz zu.

> Vgl. BVerfGE 133, 277 <311>; 141, 220 <261> zuletzt BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 99.

Ein solcher Fall liegt hinsichtlich der Befugnisse des § 11 Abs. 1a i.V.m. § 3 Abs. 1 G 10 vor. Es handelt sich um eine Maßnahme, deren Kenntnis sich den Betroffenen entzieht. Eine vorherige Benachrichtigung der einzelnen Betroffenen erfolgt nicht. Zwar findet die Regelung des § 12 Abs. 1 Satz 1 G 10 Anwendung, die eine nachträgliche Mitteilung vorsieht. Diese enthält jedoch weit gefasste Ausschlusstatbestände, welche die Benachrichtigung oftmals entfallen lassen oder langfristig aufschieben (siehe hierzu **D.I.3.c)(2)**).

Darüber hinaus ist nicht sichergestellt, dass auch Nebenbetroffene, also Dritte, die in Kontakt mit überwachten Personen stehen, von der Mitteilungspflicht des § 12 Abs. 1 Satz 1 G 10 erfasst werden. Insbesondere für die Beschwerdeführer*innen zu 1 bis 4 ist dies jedoch von großer Bedeutung, da gerade sie regelmäßig mit hoher Wahrscheinlichkeit nicht selbst Zielperson der nachrichtendienstlichen Überwachungsmaßnahmen sind, sondern vielmehr nebenbetroffene Kommunikationspartner*innen.

Die Vorschrift selbst enthält zu Dritten keine Regelungen (anders beispielsweise § 101 Abs. 4 bis 6 StPO) was auch in der Literatur auf Kritik stößt,

> *Roggan*, G 10, 2. Online-Aufl. 2018, § 12 Rn. 3; *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 12 Rn. 11 f.; *Huber*, in: Erbs/Kohlhaas, G 10, 239. EL Dezember 2021, § 12 Rn. 4.

Angesichts des Fehlens einer klaren Regelung ist nicht zweifelhaft, dass auch Nebenbetroffene benachrichtigt werden.

Als Ergebnis würden die Beschwerdeführer*innen zu 1 bis 5 und 7 lediglich ein allgemeines Schreiben mit dem Inhalt erhalten, dass kein Verstoß gegen Art. 10 Abs. 1 GG festgestellt werden konnte.

Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 15 Rn. 40.

Eine noch konkretere Darlegung der voraussichtlichen Betroffenheit ist den Beschwerdeführer*innen zu 1 bis 5 und 7 aufgrund der verdeckten Durchführung der Überwachungsmaßnahmen nicht möglich; dies hat dementsprechend auch das angerufene Gericht zur Frage der Betroffenheit durch die insoweit vergleichbaren Regelungen in § 20k und § 20l Abs. 2 des Bundeskriminalamtsgesetzes (BKAG) nicht für erforderlich gehalten.

Vgl. BVerfGE 141, 220 <262>.

2. Übermittlungsbefugnisse und das nachrichtendienstliche Informationssystem (Beschwerdeführer*innen 1 bis 5 und 7)

a) Verfassungsrechtliche Rügen

Die Beschwerdeführer*innen zu 1 bis 5 und 7 rügen zudem eine Verletzung ihrer Grundrechte durch die Übermittlungsbefugnisse des § 4 Abs. 4 Satz 1 und 2 G 10 sowie durch das nachrichtendienstliche Informationssystem, § 6 Abs. 1 und 2 BVerfSchG und § 3 Abs. 3 MADG.

Konkret verletzen die Übermittlungsbefugnisse des § 4 Abs. 4 G 10 dieselben Grundrechte, wie bereits die Erhebungsbefugnisse des § 11 Abs. 1a G 10, namentlich das Fernmeldegeheimnis, Art. 10 Abs. 1 GG, und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Diese Grundrechte werden auch durch die Übermittlungsbefugnisse nach § 4 Abs. 4 Satz 1 und Satz 2 G 10 verletzt.

Die Vorschriften zum nachrichtendienstlichen Informationssystem verletzen das Recht der Beschwerdeführer*innen zu 1 bis 5 und 7 auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Zudem sind die Regelungen auch an den Maßstäben der Grundrechte zu messen, durch die die Daten ursprünglich erhoben wurden.

b) Eigene, gegenwärtige und unmittelbare Beschwer

Die eigene, gegenwärtige und unmittelbare Betroffenheit der Beschwerdeführer*innen zu 1 bis 5 und 7 auch durch das nachrichtendienstliche Informationssystem (§ 6 BVerfSchG und § 3 Abs. 3 MADG) und die Übermittlungspflicht an Gefahrenabwehr- und Strafverfolgungsbehörden (§ 4 Abs. 4 Satz 1 G 10) ergibt sich daraus, dass die Beschwerdeführer*innen zu 1 bis 5 und 7 mit gegenüber der Allgemeinbevölkerung erhöhter Wahrscheinlichkeit Ziel von Überwachungsmaßnahmen der Nachrichtendienste sind oder aber zumindest als Kontaktperson von derartigen Maßnahmen miterfasst werden.

§ 6 Abs. 1 und 2 BVerfSchG erfasst auch Daten aus Maßnahmen des Artikel 10-Gesetzes. Denn dort ist unspezifisch die Rede von „Informationen“ der am Informationssystem teilnehmenden Behörden, wozu nach § 6 Abs. 2 Satz 2 BVerfSchG i.V.m. § 3 Abs. 3 Satz 2 MADG nun auch der MAD gehört. Darüber hinaus ist zwar nach § 4 Abs. 1 Satz 2 G 10 eine Löschung von nicht erforderlichen Daten möglich, allerdings kann die Löschung denklogisch nicht die ursprüngliche zeitlich begrenzte Speicherung ungeschehen machen.

Sobald Daten über sie erfasst wurden, besteht auch die Gefahr, dass die Daten in das Informationssystem eingespeist oder an andere Behörden gem. § 4 Abs. 4 G 10 übermittelt werden. Das umfasst auch Datenerhebungen, bei denen die Beschwerdeführer*innen lediglich als Kontaktperson erfasst wurden, § 6 Abs. 2 i.V.m. § 10 Abs. 2 Satz 1 BVerfSchG und § 4 Abs. 5 Satz 1 G 10.

Eine Möglichkeit, gegen einzelne Speicherungen oder Übermittlungen vorzugehen, besteht nicht, da hierüber keine Benachrichtigung stattfindet.

[redacted]

[redacted]

Zur Unmittelbarkeit der Betroffenheit durch das nachrichtendienstliche Informationssystem gelten die obigen Ausführungen (hierzu **1.b)(2)**) entsprechend.

Der unmittelbaren Betroffenheit steht auch der Umstand nicht entgegen, dass der MAD in § 6 Abs. 2 Satz 2 BVerfSchG und § 3 Abs. 3 Satz 2 MADG lediglich dazu ermächtigt wird, am nachrichtendienstlichen Informationssystem teilzunehmen. Damit bedarf es zwar noch einer Umsetzung dieser Ermächtigung. Es kann den Beschwerdeführer*innen zu 1 bis 5 und 7 jedoch nicht zugemutet werden, diese abzuwarten. So ist unklar, ob eine derartige Entscheidung überhaupt öffentlich bekanntgegeben wird. Darüber hinaus ist ausgeschlos-

sen, dass die Beschwerdeführer*innen zu 1 bis 5 und 7 diese Entscheidung, die nicht ihnen gegenüber ergeht und lediglich eine Vorstufe zu Grundrechtseingriffen ihnen gegenüber darstellt, angreifen könnten.

3. Fehlendes Schwachstellenmanagement (sämtliche Beschwerdeführer*innen)

Sämtliche Beschwerdeführer*innen rügen zudem die Verletzung der objektivrechtlichen Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Sinne des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Mit Ausnahme des Beschwerdeführers zu 5 sind alle Beschwerdeführer*innen hiervon in besonders gravierender Form betroffen.

a) Verfassungsrechtliche Rüge

Die Verletzung des Rechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme der Beschwerdeführer*innen in seiner Ausformung als Schutzpflicht liegt darin begründet, dass der Gesetzgeber zwar Möglichkeiten und damit Anreize geschaffen hat, Sicherheitslücken informationstechnischer Systeme zu Zwecken der Überwachung zu nutzen, nicht aber zugleich Regeln dafür aufgestellt hat, unter welchen Umständen derartige Sicherheitslücken den Hersteller*innen und Betreiber*innen der informationstechnischen Systeme bekanntgegeben werden müssen, damit diese die Lücken schließen. Auch diese Möglichkeit der Verletzung der Schutzpflicht der Beschwerdeführer*innen ist nicht aufgrund der Regelung des § 3b Abs. 1 Satz 1 oder Abs. 2 Satz 1 G 10 von vornherein ausgeschlossen (hierzu bereits **1.b)(1)(a)** und **1.b)(1)(b)**).

Das angerufene Gericht stellt an die Darlegung der Möglichkeit einer Grundrechtsverletzung besondere Anforderungen, wenn die Verletzung einer Schutzpflicht gerügt wird. Erforderlich ist es, den gesetzlichen Regelungszusammenhang insgesamt zu erfassen, wozu zumindest gehört, dass die einschlägigen Regelungen des als unzureichend beanstandeten Normkomplexes

jedenfalls in Grundzügen dargestellt werden und begründet wird, warum vom Versagen der gesetzgeberischen Konzeption auszugehen ist.

BVerfGE 158, 170 <191 f. Rn. 51>.

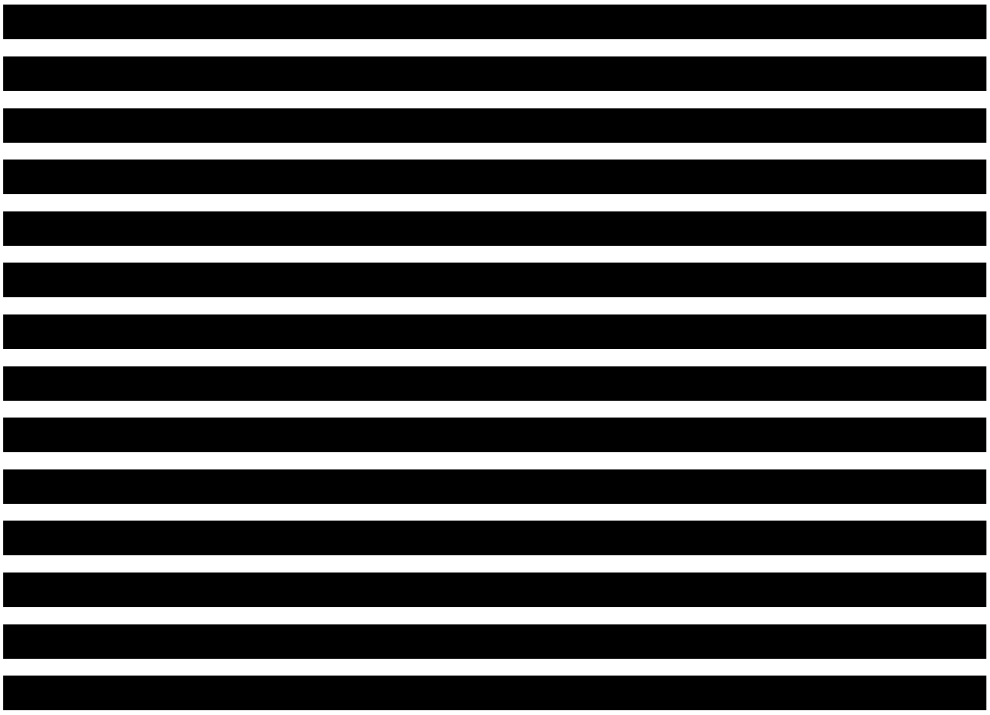
Diese geforderte ausführliche Darlegung des unzureichenden bestehenden Normkomplexes erfolgt in der Begründetheit. Es fehlen erforderliche Schutzmechanismen, sodass die gesetzgeberische Konzeption nicht den verfassungsrechtlichen Anforderungen genügt (hierzu **D.III.3.b)**).

b) Eigene, gegenwärtige, unmittelbare Betroffenheit

(1) Eigene und gegenwärtige Betroffenheit

Die Beschwerdeführer*innen sind selbst und gegenwärtig von der Schutzpflichtverletzung betroffen. Sie nutzen regelmäßig informationstechnische Systeme und sind dabei in besonderem Maße auf die Sicherheit der Systeme angewiesen.

(a) Beschwerdeführer*innen zu 1, 2 und 6



[redacted]

(b) Beschwerdeführer zu 3 und 4, 7 bis 9

[redacted]

[redacted]

[redacted]

[redacted]

(c) Beschwerdeführer zu 10

[redacted]

[redacted]

(d) Allgemeines Interesse an Datensicherheit

[redacted]

Schließlich ist zu beachten, dass insbesondere eine hohe Wahrscheinlichkeit besteht, von den besonders kritischen Zero-Day-Schwachstellen betroffen zu sein. Wenn für diese bereits ein funktionierender Angriffscode existiert, besteht eine große Wahrscheinlichkeit einer breiten Ausnutzung und mithin einer eigenen und gegenwärtigen Betroffenheit. Dass dies kein unwahrschein-

liches Szenario ist, macht bereits folgendes Beispiel deutlich: Im Berichtszeitraum 2021 des Bundesamts für Sicherheit in der Informationstechnik (BSI) hatte insbesondere die Schwachstelle *Proxylogon* (CVE-2021-26855) eine solche Charakteristik, welche den weit verbreiteten Microsoft Groupware- und E-Mail-Server *Exchange* betraf. Im März 2021 nutzten Hacker*innen diese aus, um Zugriff auf betroffene Systeme zu erhalten, E-Mails auszuspähen oder Schadprogramme, wie Ransomware, auszurollen. Zum Zeitpunkt des Bekanntwerdens der Schwachstellen waren 98 % der geprüften Systeme in Deutschland verwundbar. Daraufhin stufte das BSI die Bedrohungslage als extrem kritisch ein und stellte regelmäßig aktualisierte Sicherheitsinformationen bereit. Nichtsdestotrotz waren noch im Mai 2021 knapp 9 % der geprüften Exchange-Server in Deutschland für die kritischen Schwachstellen verwundbar.

> Vgl. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2021, S. 26 f., abrufbar unter https://www.bsi.bund.de/DE/ServiceNavi/Publikationen/Lagebericht/lagebericht_node.html.

Veranschaulicht wird das Risiko zudem durch die nach wie vor vielerorts vorzufindende und häufig für Angriffe verwendete Schwachstelle *Bluekeep* (CVE-2019-0708) in Microsofts Remote Desktop Protocol, die Angreifer*innen ermöglicht, beliebige Codes wie etwa Schadprogramme auf dem schwachstellenbehafteten System auszuführen.

> Vgl. Microsoft 'Bluekeep' Flaw Threatens Medical Devices, IoT, virsec vom 4. Juni 2019, abrufbar unter: https://www.virsec.com/blog/microsoft-bluekeep-flaw-threatens-medical-devices-iot.

Schließlich zeigt auch das Schadprogramm *WannaCry* die Risiken auf, die mit der Verheimlichung von Sicherheitslücken einhergeht. Das Programm hat im Mai 2017 weltweit erhebliche Schäden verursacht, indem es betroffene Systeme lahmlegte und nur gegen Lösegeldzahlung wieder freigab. Die Sicherheitslücken, welche die hinter *WannaCry* stehenden Kriminellen ausnutzten,

waren zuvor der amerikanischen National Security Agency (NSA) gestohlen worden.

> Vgl. etwa Microsoft gibt US-Regierung Mitschuld an Hackerangriff, Zeit, vom 15. Mai 2017, abrufbar unter https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung.

Diese Beispiele veranschaulichen die akut hohe Gefährdungslage der IT-Sicherheit in Deutschland (hierzu ausführlich **D.III.2.a)**) und verdeutlichen die große Wahrscheinlichkeit einer eigenen und gegenwärtigen Betroffenheit der Beschwerdeführer*innen.

(2) Unmittelbare Betroffenheit

Die Ermächtigungen der § 11 Abs. 1a i.V.m. § 3 Abs. 1 G 10 betreffen alle Beschwerdeführer*innen auch unmittelbar, weil es zu ihrer Beschwer keines weiteren gegen sie gerichteten Akts bedarf.

Vielmehr folgt ihre Betroffenheit gerade aus der signifikant erhöhten Dauergefahr, die daraus resultiert, dass die Nachrichtendienste ihnen bekanntwerdende Sicherheitslücken unter Verletzung der Schutzpflicht des Staates gegenüber den Beschwerdeführer*innen nicht an die Hersteller*innen der betroffenen Programme und informationstechnischen Systeme melden. Außerdem ist zu beachten, dass die Beschwerdeführer*innen mangels Kenntnis eines möglichen Vollzugaktes – wenn der Staat Kenntnis von Sicherheitslücken erhält und diese geheim hält – nicht vorgehen können.

III. Rechtswegerschöpfung und Subsidiarität

Zunächst steht unmittelbar gegen die angegriffenen Parlamentsgesetze kein Rechtsweg im Sinne des § 90 Abs. 2 BVerfGG zur Verfügung, welcher vor Erhebung der Verfassungsbeschwerde erschöpft werden könnte.

Darüber hinaus steht der Grundsatz der Subsidiarität der Zulässigkeit der vorliegenden Verfassungsbeschwerde nicht entgegen. Grundsätzlich erfordert dieser, dass vor Einlegung einer Verfassungsbeschwerde alle zur Verfügung stehenden prozessualen Möglichkeiten zu ergreifen sind. Derartige Möglichkeiten bestehen vorliegend nicht.

1. Quellen-Telekommunikationsüberwachung und beschränkte Online-Durchsuchung

Die Beschwerdeführer*innen zu 1 bis 5 und 7 erhalten von den staatlichen Maßnahmen nach den angegriffenen Vorschriften in der Regel keine Kenntnis. Indem regelmäßig die Mitteilungen nach § 12 Abs. 1 Satz 1 G 10 unterbleiben, ist nicht garantiert, dass sich die Beschwerdeführer*innen gegen sie betreffende Maßnahmen richten können, sei es auch nur im Nachhinein.

> Vgl. etwa BT-Drs. 19/163, S. 6; 18/11227, S. 6 (im Berichtszeitraum unterblieb in etwa 75 % der Fälle eine Mitteilung); *Roggan*, G 10, 2. Online-Aufl. 2018, § 12 Rn. 4.

a) Kein vorbeugender Rechtsschutz

Ein vorbeugender Rechtsschutz in Gestalt einer vorbeugenden Unterlassungs- oder Feststellungsklage ist den Beschwerdeführer*innen zu 1 bis 5 und 7 nicht eröffnet. Solche Klagen setzen nach gefestigter Rechtsprechung voraus, dass sich ein drohendes Verwaltungshandeln bzw. ein zukünftiges Rechtsverhältnis bereits hinreichend konkret abzeichnet und die für eine Rechtmäßigkeitsprüfung erforderliche Bestimmtheit aufweist.

Vgl. zur vorbeugenden Unterlassungsklage BVerwG, Urteil vom 19. März 1974 – 1 C 7.73; Beschluss vom 30. September 1981 – 3 B 39.81; Urteil vom 13. Dezember 2017 – 6 A 6.16 Rn. 12; *Pietzcker/Marsch*, in: Schoch/Schneider, VwGO, 41. EL Juli 2021, § 42 Abs. 1 Rn. 163; zur Feststellungsklage BVerwG, Urteil vom 17. Januar 1980 – 7 C 63.77; Urteil vom 7. Mai 1987 – 3 C 53/85; Urteil vom 30. Mai 2018 – 6 A 3/16 Rn. 53 f.; *Pietzcker*, in: Schoch/Schneider, VwGO, 41. EL Juli 2021, § 43 Rn. 32.

Eine konkrete Bestimmung drohender Überwachungsmaßnahmen oder eines Informationsaustauschs ist den Beschwerdeführer*innen zu 1 bis 5 und 7 jedoch nicht möglich. Hierzu müssten diese Beschwerdeführer*innen zu 1 bis 5 und 7 ein konkretes behördliches Verfahren bezeichnen können, in dessen Rahmen ihnen eine Überwachung droht. Aus ihrer Betroffenenperspektive lassen sich solche Verfahren im Voraus aber nicht absehen.

Um Rechtsschutz gegen die Maßnahmen zu erlangen, bliebe den Beschwerdeführer*innen zu 1 bis 5 und 7 regelmäßig lediglich eine vorbeugende Klage gegen unbestimmte Überwachungsmaßnahmen in unbestimmten Verfahren. Eine solche Klage ins Blaue hinein sprengte jedoch den in langjähriger Rechtsprechung entwickelten Rahmen des vorbeugenden Rechtsschutzes und wäre daher unzulässig.

Ein derartiges Vorgehen scheitert zudem bereits an § 13 G 10, nach dem Rechtsschutz vor einer Mitteilung über eine Maßnahme – und damit auch den vorbeugenden Rechtsschutz – ausgeschlossen ist.

Selbst wenn dies anders zu sehen wäre, wäre ein solcher Rechtsschutz so inadäquat, dass der Subsidiaritätsgrundsatz nicht dazu zwingen könnte, ihn vorrangig zu ergreifen. Soweit nämlich die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es keiner vorangehenden fachgerichtlichen Entscheidung.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 Rn. 102; BVerfGE 143, 246 <321 f. Rn. 210>; 145, 20 <54 f. Rn. 85 f.>; 150, 309 <326 f. Rn. 42 ff.>; 158, 170 Rn. 68 ff.; zuletzt BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 102 stRspr.

So läge der Fall bei einer vorbeugenden Unterlassungs- oder Feststellungsklage gegen verdeckte Überwachungsmaßnahmen nach den angegriffenen Regelungen.

Da die Beschwerdeführer*innen zu 1 bis 5 und 7 konkrete Überwachungsanlässe im Voraus nicht absehen und nicht benennen können, müsste eine solche Klage darauf gerichtet sein, eine Überwachung der Beschwerdeführer*innen nach den angegriffenen Regelungen generell zu unterlassen. Diese Klage wäre nur begründet, wenn es keinen denkbaren Sachverhalt gäbe, in dessen Rahmen die Beschwerdeführer*innen zu 1 bis 5 und 7 einer solchen Überwachung ausgesetzt werden dürften. Dies ließe sich nur annehmen, wenn die angegriffenen Regelungen auch bei restriktiver Interpretation und unabhängig von ihrer tatsächlichen Handhabung verfassungswidrig wären. Ausführungen zur Auslegung und Anwendung der Normen könnten die Fachgerichte daher allenfalls als *obiter dicta* machen, zu denen sie nicht gehalten sind und deren bloße Möglichkeit unter Subsidiaritätsgesichtspunkten keinen fachgerichtlichen Rechtsschutz gebieten kann. Vielmehr wäre eine Aufklärung der einfachrechtlichen Rechtslage und der tatsächlichen Gegebenheiten im Verwaltungsprozess nicht angezeigt. Das verwaltungsgerichtliche Verfahren wäre vielmehr materiell als reiner Verfassungsprozess zu führen, was der Subsidiaritätsgrundsatz gerade nicht verlangt.

Vgl. BVerfGE 123, 148 <172 f.>; 143, 246 <322>; 150, 309 Rn. 44 stRspr.

Schließlich ist es den Beschwerdeführer*innen auch nicht zumutbar fachgerichtlichen Rechtsschutz geltend zu machen. Dies ergibt sich bereits aus dem Umstand, dass nach § 1 Abs. 1 G 10 insgesamt 19 Behörden ermächtigt werden. Die Beschwerdeführer*innen müssten mithin gegen all diese vor insgesamt 17 Gerichten vorgehen, um sicherzustellen, dass sie ihre Rechtsschutz-

ziele erreichen. Damit wäre ein unverhältnismäßiger Aufwand verbunden. Zudem würde dies zu der besonderen Situation führen, dass nicht all diese Verfahren zum selben Zeitpunkt enden und damit auch nicht einheitlich Verfassungsbeschwerde erhoben werden könnte. Durch diese zeitliche Zerstückelung des Rechtsschutzes wird aber zugleich der Gedanke der weiteren fachgerichtlichen Aufklärung konterkariert, da zum Zeitpunkt der ersten Verfassungsbeschwerde noch gar nicht deutlich sein wird, wie in anderen Verfahren entschieden wird. Zugleich müsste bereits aufgrund der Frist des § 93 Abs. 1 Satz 1 BVerfGG zeitnah Verfassungsbeschwerde erhoben werden.

b) Unzureichender nachträglicher Rechtsschutz

Eine vorherige fachgerichtliche Befassung ist auch mit Blick auf die Überprüfung der Verfassungskonformität der weitreichenden Ausnahmen von den Benachrichtigungspflichten infolge einer Beschränkungsmaßnahme unzumutbar.

Generell besteht zwar nach der Rechtsprechung des angerufenen Gerichts keine Möglichkeit der Erhebung einer Verfassungsbeschwerde unmittelbar gegen ein Gesetz, welches zu heimlichen Maßnahmen berechtigt, wenn die Betroffenen durch eine aktive Informationspflicht des Staates rechtlich gesichert später Kenntnis von der Maßnahme erlangen.

> Vgl. BVerfGE 156, 11 <35 Rn. 62>; instruktiv zu den hiesigen Vorbedingungen effektiver Rechtsschutzgewährung: *Buchberger*, in: Dietrich et al., Nachrichtendienste im demokratischen Rechtsstaat – Kontrolle – Rechtsschutz – Kooperationen, 1. Aufl. 2018, 107 (110 ff.).

Ist die Kenntniserlangung jedoch nicht hinreichend abgesichert, kann im Umkehrschluss auch der Grundsatz der Subsidiarität keine vorherige fachgerichtliche Klärung erfordern. In Anbetracht der weitreichenden Ausnahmetatbestände nach § 12 Abs. 1 Satz 2 G 10 erfolgt eine solche ausreichend rechtlich gesicherte spätere Kenntniserlangung gerade nicht.

Zunächst sind die Voraussetzungen der Ausnahmetatbestände § 12 Abs. 1 Satz 2 G 10 zu unbestimmt formuliert, was ein Unterlassen der Benachrichtigung in nahezu jedem Fall möglich macht. Beispielweise wird nicht deutlich unter welchen Umständen eine „Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann“ (hierzu ausführlich **D.I.3.c)(2)**). Zudem ist die Vorschrift zu weit gefasst, die Ausnahme wird aufgrund der weitgehenden Einschränkung der Mitteilungspflicht zur Regel umgekehrt, was insbesondere in der Geheimhaltungsquote von 75 % zum Ausdruck kommt (hierzu **II.1.b)(2)**).

> Vgl. BT-Drs. 19/163, S. 6; 18/11227, S. 6; *Roggan*, G 10, 2. Online-Aufl. 2018, § 12 Rn. 4.

Damit wird Betroffenen faktisch das Recht genommen, sich – wenn auch nur im Nachhinein – gegen eine Maßnahme zur Wehr zu setzen. Es besteht daher die begründete Besorgnis, dass im Regelfall der Weg zur fachgerichtlichen Klärung der Reichweite der Ausnahmetatbestände anhand einer zunächst zurückgehaltenen, aber nachgeholten Benachrichtigung versperrt bleibt. Dies ist nicht mit dem Gebot effektiven Rechtsschutzes des Art. 19 Abs. 4 GG zu vereinbaren.

Darüber hinaus besteht zwar die Möglichkeit, dass eine zunächst zurückgestellte Benachrichtigung zu einem späteren Zeitpunkt noch erfolgt. Allerdings bliebe es für die Zulässigkeit einer Verfassungsbeschwerde dem bloßen und für die Beschwerdeführer*innen nicht abschätzbaren Zufall überlassen, ob bis zu fünf Jahre (§ 12 Abs. 1 Satz 3 Nr. 1 G 10) nach der konkreten Maßnahme eine Benachrichtigung doch noch erfolgt oder mit Zustimmung der G 10-Kommission von dieser abgesehen wird. Auch bei Einhaltung der – bereits zu weit und zu unbestimmt formulierten – Voraussetzungen des § 12 Abs. 1 Satz 2 G 10 kommen also noch weitere, zu weitgehende Einschränkungen zum Tragen (§ 12 Abs. 1 Satz 3 und 4 G 10).

> Vgl. *Wollweber*, ZRP 2001, 213 (216); *Bergemann*, in: Lisken/Denninger, PolR-HdB, H. Nachrichtendienste und Polizei Rn. 180;

Bantlin, Die G10-Kommission – Zur Kontrolle der Nachrichtendienste, 1. Aufl. 2021, S. 162 f.

Durch die Verzögerung der Mitteilung können sich im Falle einer zu Unrecht unterlassenen Benachrichtigung gravierende Einbußen im Rechtsschutz der Betroffenen ergeben. Das Ergreifen von Rechtsschutz ist nämlich – wenn überhaupt – erst nach einer Mitteilung möglich (§ 13 G 10).

Vgl. VG Wiesbaden Beschluss vom 24. November 2021 – 6 L 1358/21.WI, Rn. 42 ff.

All diese Aspekte machen die Notwendigkeit eines unmittelbaren Vorgehens gegen das Gesetz im Wege einer Verfassungsbeschwerde deutlich.

Hinzu kommt, dass die Vorschriften eine Vielzahl an Adressaten ermächtigen. Konkret sind dies gemäß § 1 Abs. 1 G 10 die Verfassungsschutzbehörden des Bundes und der Länder, der Bundesnachrichtendienst (BND) und der MAD. Es wären mithin Klagen gegen 19 verschiedene Behörden vor 17 verschiedenen Gericht notwendig, um eine Überwachungsmaßnahme sicher ausschließen zu können. Ein Vorgehen gegen nur einzelne Behörden hätte zur Gefahr, dass andere Behörden – sei es aufgrund landesrechtlicher Besonderheiten – eine andere Auffassung der rechtlichen Rahmenbedingungen annehmen. Erschwerend kommt hinzu, dass das Gesetz auch den BND ermächtigt, dessen Aufgabenspektrum sich aber von dem der Inlandsnachrichtendienste unterscheidet. Dies erhöht die Gefahr divergierender Gerichtsentscheidungen.

c) Kein Schutz durch G 10-Kommission

Schließlich würde auch eine Beschwerde bei der G 10-Kommission keine Abhilfe schaffen, da sich die Beschwerdeführer*innen zu 1 bis 5 und 7 grundlegend gegen die Verfassungsmäßigkeit der Rechtsgrundlage der Beschränkungsmaßnahmen richten und nicht gegen eine konkrete Entscheidung im Einzelfall. Diese Frage kann die G 10-Kommission weder selbst klären, noch kann sie – wie etwa die Gerichte – eine konkrete Normenkontrolle nach Art.

100 Abs. 1 GG einleiten, um die Verfassungsmäßigkeit der Regelungen vom angerufenen Gericht klären zu lassen.

2. Schutzpflichtverletzung

In Bezug auf die Rüge der Schutzdimension steht sämtlichen Beschwerdeführer*innen keine andere Möglichkeit zu, Rechtsschutz zu erlangen.

Das angerufene Gericht hat in der Vergangenheit betont, der Grundsatz der Subsidiarität gebiete auch bei der Rüge einer objektiven Schutzpflichtverletzung die Möglichkeit der sich aus der der vorbeugenden Unterlassungsklage sowie der Feststellungsklage ergebenden Möglichkeiten auszuschöpfen.

> BVerfGE 158, 170 <199 Rn. 70>.

In Bezug auf die Rüge der Verletzung der objektiven Schutzpflicht ist dies im hiesigen Verfahren bei genauerer Betrachtung jedoch aussichtslos und folglich unzumutbar. Die Beschwerdeführer*innen begehren vorliegend die erstmalige Entwicklung und Implementierung eines behördlichen Schwachstellenmanagements. Die vorgenannten Verfahrensarten vermögen dieses Ziel nicht zu erreichen.

Dies gilt zunächst für ein Vorgehen im Wege einer allgemeinen Leistungsklage, die einzelnen Nachrichtendienste für die Zukunft konkret zu verpflichten, zur Kenntnis gelangte Sicherheitslücken zu melden bzw. offenzulegen. Ein einfachgesetzlicher Anspruch auf ein solches schlicht-hoheitliches Handeln ist nicht normiert, sodass eine entsprechende Klage mangels Klagebefugnis entsprechend § 42 Abs. 2 VwGO unzulässig wäre. Denn die gesetzlich vorgesehenen Meldepflichten der Nachrichtendienste gegenüber dem BSI gem. § 4 Abs. 3 BSIG (hierzu im Einzelnen unten bei **D.III.3.b)(3)**) sind nicht den Individualinteressen der Beschwerdeführer*innen zu dienen bestimmt, sondern stellen sich als interbehördliche Verfahrensregelung zum Meldesystem dar.

> Vgl. BT-Drs. 16/11967, S.13.

Auch ein grundrechtlich fundierter Anspruch auf eine Meldung bzw. Offenlegung von Schwachstellen besteht nicht, wie das angerufene Gericht in der Vergangenheit bereits deutlich gemacht hat.

Vgl. BVerfGE 158, 170 <189 Rn. 43>.

Der Versuch einer Klärung im Rahmen des Vorgehens gegen konkrete Überwachungsmaßnahmen im Wege der vorbeugenden Unterlassungsklage erscheint ebenso wenig erfolgversprechend. Dem steht erstens § 13 G 10 entgegen, der kategorisch den vorbeugenden Angriff der Anordnung einer Beschränkungsmaßnahme ausschließt. Zweitens wird selbst unter Ausklammerung der Rechtswegbeschränkung kein anderes Ergebnis erreicht. Geht eine konkret durch eine Überwachungsmaßnahme bedrohte Personen gegen die Maßnahme vor, besteht der Streitgegenstand nicht in der zeitlich vorgelagert unterbliebenen Abwägung über die Meldung der Schwachstelle, sondern lediglich in der Zulässigkeit des konkret-individuellen Einsatzes der Überwachungsmittel. Wird hingegen von den durch das Offenhalten betroffenen Repräsentanten der Allgemeinheit ausgegangen, so wären diese mangels qualifizierten Rechtsschutzbedürfnisses nicht klagebefugt, da eine drohende Überwachung im Regelfall nicht dargelegt werden könnte.

Eine Klage auf Feststellung, dass die Grundrechte weitere Vorkehrungen zur hinreichenden Berücksichtigung des Schutzes solcher Systeme vor Infiltrationen durch Dritte bei Entscheidungen über die Offenhaltung unerkannter Sicherheitslücken für etwaige Quellen-Telekommunikationsüberwachungen gebieten, ist letztlich ebenso aussichtslos, wie eine Klage auf vorbeugende Negativfeststellung, wonach das Offenhalten bestimmter Zero-Day-Schwachstellen unzulässig wäre. Diese Klagen wären mit Blick auf die Sachurteilsvoraussetzung des Gegenstands der Feststellung offensichtlich unzulässig.

Eine Feststellungsklage setzt gem. § 43 Abs. 1 VwGO ein feststellungsfähiges Rechtsverhältnis voraus. Unter einem Rechtsverhältnis sind die rechtlichen Beziehungen zu verstehen, die sich aus einem konkreten Sachverhalt aufgrund einer öffentlich-rechtlichen Norm für das Verhältnis von natürlichen oder juristischen Personen untereinander oder einer Person zu einer Sache ergeben.

Die Beteiligten müssen über die Anwendung einer Rechtsnorm auf einen bestimmten, überschaubaren, gerade auch die jeweiligen Kläger*innen betreffenden Sachverhalt streiten und dürfen den Verwaltungsgerichten nicht lediglich abstrakte Rechtsfragen, die sich auf der Grundlage eines nur erdachten oder als möglich vorgestellten Sachverhalts stellen, zur Klärung vorlegen.

> Vgl. BVerwGE 14, 235 [236]; 157, 126 [128 f.], stRspr.

Bei der Frage, ob weitere behördliche Vorkehrungen zum Schutz informationstechnischer Systeme geboten sind, handelt es sich nicht um ein konkretisiertes Rechtsverhältnis, da sich die Feststellung nicht auf einen bestimmten, bereits überschaubaren Sachverhalt beschränkt, sondern auf einen bloß potenziellen Sachverhalt bezieht. Eine hinreichend konkrete rechtliche Beziehung läge der Feststellung nur dann zugrunde, wenn mit an Sicherheit grenzender Wahrscheinlichkeit feststünde, dass die von den Beschwerdeführer*innen genutzten informationstechnischen Systeme von denjenigen Sicherheitslücken betroffen sind, die zugleich vom jeweiligen Nachrichtendienst nachweislich zur Infiltration eines informationstechnischen Systems temporär offengehalten wurden. Ist es wie hier indes lediglich möglich oder denkbar, dass zu irgendeinem Zeitpunkt eine schwachstellenbezogene Kongruenz zwischen individueller Betroffenheit und Offenhaltungsentscheidung bestand oder besteht, so genügt dies nicht den Konkretisierungsanforderungen im Verwaltungsprozess, da es sich um eine unzulässige Klärung abstrakter Rechtsfragen handeln würde.

> Vgl. BVerwG, Urteil vom 28. Mai 2014 – 6 A 1/13 –, Rn. 20; Urteil vom 14. Dezember 2016 – 6 A 9/14 –, Rn. 12.

Hinsichtlich der Negativfeststellung, dass eine Zero-Day-Schwachstelle nicht offengehalten werden dürfte, erscheint es ebenfalls ausgeschlossen, dass das Rechtsverhältnis im fachgerichtlichen Verfahren hinreichend konkretisiert werden könnte, damit es den Sachurteilsvoraussetzungen noch genügt. Die Konkretisierung auf eine bestimmte Sicherheitslücke ist den betroffenen Beschwerdeführer*innen gerade nicht möglich, da diese erst mit Veröffentlichung und nicht vor der bewussten Offenhaltung von einer solchen erfahren.

Selbst nach dem Bekanntwerden von Sicherheitslücken ist für die Betroffenen der Umgang mit Schwachstellen aufgrund der Klassifizierung der Vorgänge nicht einsehbar.

Überdies wäre aber auch keine weitergehende Aufklärung durch fachgerichtlichen Rechtsschutz zu erwarten. Es bestehen gerade keine ernstzunehmenden Ansätze für ein Schwachstellenmanagement auf Bundesebene. Es existieren weder spezifische Regelungen für den beschriebenen Zielkonflikt, noch bestehen hinreichende Vorschriften zur Datenschutz-Folgeabschätzung, zu den Befugnissen des BSI und zur sonstigen IT-Sicherheitsarchitektur des Bundes. Auch im Europa- und Völkerrecht und in landesrechtlichen und untergesetzlichen Regelungen ist offensichtlich kein erforderliches gesetzliches Schwachstellenmanagement zu finden (siehe hierzu bereits **a)** und ausführlich **D.III.3.b)**). Die existierenden Regelungen sind offensichtlich ungeeignet, den verfassungsrechtlichen Anforderungen zu genügen, weshalb kein Bedürfnis für eine fachgerichtliche Befassung mit den zugrundeliegenden Rechtsfragen besteht. Vielmehr kann bereits innerhalb dieser Verfassungsbeschwerde die Evidenz der Mangelhaftigkeit der bestehenden Vorschriften aufgezeigt werden.

Folglich wirft die Beurteilung der angegriffenen Normen allein verfassungsrechtliche Fragen auf, ohne dass durch eine vorausgegangene fachgerichtliche Prüfung einer verbesserte Entscheidungsgrundlage zu erwarten wäre. Es gilt also vom angerufenen Gericht zu klären, welche konkreten Anforderungen an ein Schwachstellenmanagement sich aus der Schutzpflicht aus dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergeben.

Schließlich ist für den fachgerichtlichen Rechtsschutz nach oben zu verweisen. Da 19 Behörden ermächtigt werden, ist ein vorbeugendes Vorgehen unzumutbar.

3. Informationssystem und Übermittlungsbefugnis

Etwas anderes ergibt sich auch nicht hinsichtlich des nachrichtendienstlichen Informationssystems sowie der Übermittlungsbefugnisse des § 4 Abs. 4 G 10.

Betroffene bekommen nicht mitgeteilt, dass eine Speicherung im Informationssystem erfolgt oder Daten aus diesem genutzt werden bzw. erhobene Daten nach § 4 Abs. 4 G 10 an andere Stellen übermittelt werden. Regelmäßig werden diese nicht einmal wissen, dass überhaupt Daten über sie erhoben wurden. Damit scheidet ein Vorgehen gegen eine konkrete Speicherung, Nutzung oder Übermittlung aus.

Auch vorbeugender Rechtschutz in Form einer vorbeugenden Unterlassens- oder einer Feststellungsklage scheitern vorliegend. So müsste ein Unterlassens- oder Feststellungsantrag darauf gerichtet sein, dass keine Speicherung, keine Nutzung oder keine Übermittlung von Daten stattfinden dürfte. Dazu müssten diese aber in jedweder Situation ausgeschlossen sein. Das ist jedoch nicht der Fall.

Auch hier besteht zudem das Problem der besonderen Weite der Ermächtigungen. So umfasst das nachrichtendienstliche Informationssystem mit Ausnahme des BND alle Nachrichtendienste, § 4 Abs. 4 G 10 sogar sämtliche Nachrichtendienste. Da es gerade um unbekannte Fälle geht, wäre damit ebenfalls ein Vorgehen gegenüber all diesen Diensten notwendig, was den Beschwerdeführer*innen zu 1 bis 5 und 7 nicht zuzumuten ist.

In Bezug auf das nachrichtendienstliche Informationssystem stellt auch die Beschwerde an den*die Bundesbeauftrage*n für den Datenschutz und die Informationsfreiheit gem. § 28 Abs. 1 BVerfSchG dar. Hier bestehen die gleichen Probleme, dass nicht bekannt wird, wann es zu einer Speicherung oder Nutzung gespeicherter Daten kommt. Ein vorbeugendes Vorgehen ist nicht vorgesehen. Zudem ist nicht gesichert, dass ein derartiges Verfahren erfolgreich sein kann, da gegenüber dem*der Bundesbeauftragten Auskünfte auch in Ausnahefällen verweigert werden können, § 28 Abs. 3 Satz 3 BVerfSchG.

IV. Beschwerdefrist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Das Gesetz zur Anpassung des Verfassungsschutzrechts ist hinsichtlich der anzugreifenden Regelungen gemäß Artikel 8 Abs. 1 dieses Gesetzes am Tag nach seiner Verkündung und damit am 9. Juli 2021 in Kraft getreten. Die Jahresfrist endet folglich mit dem 8. Juli 2022.

Auch Vorschriften des Artikel 10-Gesetzes und des Bundesverfassungsschutzgesetzes, die selbst nicht unmittelbar durch das Gesetz zur Anpassung des Verfassungsschutzrechts geändert wurden, können durch das Änderungsgesetz einer Überprüfung zugeführt werden, da diese durch die neuen Regelungen eine andere Qualität erhalten haben und daher die Jahresfrist neu zu laufen beginnt.

> Vgl. BVerfGE 100, 313 <356>; 141, 220 <262 f.>.

Das betrifft zunächst die allgemeinen Regelungen des Artikel 10-Gesetzes, auf welche die neuen Befugnisse Bezug nehmen. § 3 Abs. 1G 10 und § 4 Abs. 4 Satz 1 und 2 G 10 wurden durch die Einführung der Quellen-Telekommunikationsüberwachung und der beschränkten Online-Durchsuchung in einen neuen Regelungskontext gestellt. § 11 Abs. 1a G 10 greift auf die Voraussetzungen des § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 zurück. Somit erfährt der Anwendungsbereich dieser Regelungen nicht nur eine wesentliche Erweiterung, sondern hebt sich vom bisherigen Regelungszustand auch durch neue, zusätzliche Belastungen ab.

Auch die Regelung zu den Mitteilungspflichten aus § 12 G 10 und zum partiellen Ausschluss des Rechtswegs nach § 13 G 10 können angegriffen werden, da diese als Verfahrensvorschriften auch die Eingriffsintensität der neuen Befugnisse mitbestimmen. Denn es wird den Betroffenen regelmäßig nicht möglich sein, effektive Rechtsschutzmaßnahmen gegen die getroffene Maßnahmen zu erheben, da in der Praxis regelmäßig gar nicht erst eine Mitteilung nach § 12 Abs. 1 Satz 1 G 10 erfolgt und zudem der Rechtsweg gegen die Anordnung und

den Vollzug von Beschränkungsmaßnahmen vor deren Mitteilung an den Betroffenen nach § 13 G 10 ausgeschlossen wird (hierzu bereits **II.1.b)(2)**, **III**. und ausführlich **D.I.3.c)**).

Die Gesetzesänderung bewirkt zudem eine Intensivierung des Eingriffsgewichts der Übermittlungsbefugnisse des § 4 Abs. 4 G 10. Über diesen können nunmehr auch Daten übermittelt werden, die durch die Quellen-Telekommunikationsüberwachung und die beschränkte Online-Durchsuchung übermittelt werden.

Schließlich bewirken die gesetzlichen Neufassungen auch eine Wesensänderung des nachrichtendienstlichen Informationssystems in zwei Hinsichten.

Zunächst wurden § 6 Abs. 2 BVerfSchG und § 3 Abs. 3 MADG dahingehend geändert, dass nunmehr auch der MAD am Informationssystem teilnehmen darf. Gegen diese gesetzliche Änderung gilt die Beschwerdefrist des § 93 Abs. 3 BVerfGG unmittelbar.

Darüber hinaus führt aber auch die Einführung der neuen Eingriffsbefugnisse des § 11 Abs. 1a G 10 zu einer Intensivierung des Eingriffs durch das Informationssystem. Bei den Maßnahmen handelt es sich um intensive Grundrechtseingriffe, die zur Erhebung einer Vielzahl an höchst sensiblen Daten führen kann (hierzu **D.I.1** und **D.II.1**). Auch für diese Daten gilt, dass sie aufgrund der niedrigen Speicherschwellen (hierzu **D.V.3.a)(2)(a)**) in aller Regel in das System eingespeist werden. An dieser zunächst erfolgenden Speicherung ändert auch die spätere Möglichkeit zur Löschung von nicht erforderlichen Daten nach § 4 Abs. 1 Satz 2 G 10 nichts. Dadurch intensiviert sich der Grundrechtseingriff durch das Informationssystem sowohl in quantitativer als auch in qualitativer Hinsicht. Als Konsequenz daraus muss es den Beschwerdeführer*innen entsprechend der Rechtsprechung des angerufenen Gerichts zustehen, dieses System einer verfassungsrechtlichen Überprüfung zuzuführen.

D. Begründetheit der Verfassungsbeschwerde

I. Quellen-Telekommunikationsüberwachung (§ 11 Abs. 1a Satz 1 G 10)

Die in § 11 Abs. 1a Satz 1 G 10 normierte Quellen-Telekommunikationsüberwachung verletzt das Fernmeldegeheimnis der Beschwerdeführer*innen zu 1 bis 5 und 7 aus Art. 10 Abs. 1 GG. Die Maßnahme greift intensiv in dieses Recht ein (hierzu unter **1.**), ohne verfassungsrechtlich gerechtfertigt zu sein. So ist die Ermächtigungsgrundlage bereits mangels einer Gesetzgebungskompetenz des Bundes formell verfassungswidrig (hierzu unter **2.**). Zudem verstößt § 11 Abs. 1a Satz 1 G 10 in mehrfacher Hinsicht gegen den Verhältnismäßigkeitsgrundsatz und ist damit auch materiell verfassungswidrig (hierzu unter **3.**).

1. Die Quellen-Telekommunikationsüberwachung greift intensiv in das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) ein

Das angerufene Gericht ordnet den Schutz der laufenden Telekommunikation dem Fernmeldegeheimnis zu.

> Vgl. BVerfGE 120, 274 <309>; 141, 220 <309, Rn. 228>.

Eine Überwachung der Telekommunikation greift in das Fernmeldegeheimnis ein. Ein derartiger Eingriff wiegt regelmäßig schwer.

> Vgl. BVerfGE 113, 348 <382>; 129, 208 <240>; 141, 22 <310>.

Auch bei der vorliegenden Quellen-Telekommunikationsüberwachung bestehen mehrere Umstände, die ein besonderes Eingriffsgewicht begründen.

So hat das angerufene Gericht in seiner Rechtsprechung betont, dass heimliche Überwachungsmaßnahmen sehr intensive Eingriffe in Grundrechte bewirken können. Das Eingriffsgewicht der Überwachungsmaßnahme durch

einen Nachrichtendienst hängt insbesondere davon ab, wie weitgehend die Persönlichkeit erfasst werden kann, ob besonders private Informationen erlangt werden können oder ob berechtigte Vertraulichkeitserwartungen überwunden werden. Besonders schwer wiegt danach etwa die Erfassung nichtöffentlicher Gespräche. Dabei wird das Gewicht des Eingriffs auch von der Dauer der Überwachungsmaßnahme geprägt.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 191 m.w.N.

Bereits nach diesen Maßstäben handelt es sich bei der Quellen-Telekommunikationsüberwachung um einen gewichtigen Eingriff.

Da es sich um eine heimliche Maßnahme handelt, können sich Betroffene nicht gegen die Maßnahme wehren und diese allenfalls im Nachhinein überprüfen lassen.

Die Quellen-Telekommunikationsüberwachung ermöglicht zudem die Erfassung besonders privater Informationen. Insbesondere können auch nichtöffentliche Gespräche überwacht werden, bei denen davon auszugehen ist, dass private Informationen geteilt werden.

Auch dient die Quellen-Telekommunikationsüberwachung – indem sie getroffene Schutzmaßnahmen umgeht – gerade dazu, berechtigte Vertraulichkeitserwartungen zu überwinden. Beispielsweise verwenden viele Messenger-Dienste wie WhatsApp eine Ende-zu-Ende Verschlüsselung. Gerade dieses Instrument umgeht die Quellen-Telekommunikationsüberwachung. Die Betroffenen sind den verdeckten Überwachungsmaßnahmen also gerade in einer Situation vermeintlicher Vertraulichkeit ausgesetzt. Insbesondere Kontaktpersonen oder sonstige Dritte rechnen nicht damit, Ziel von nachrichtendienstlicher Überwachung zu werden.

Auch ermöglicht die § 11 Abs. 1a Satz 1 G 10 eine Überwachung über einen unbegrenzt langen Zeitraum. Zwar kann jede einzelne Maßnahme lediglich für drei Monate angeordnet werden (§ 10 Abs. 5 Satz 1 G 10), aber Verlängerun-

gen sind nach § 10 Abs. 5 Satz 2 G 10 möglich. Eine Höchstdauer ist nicht vorgeschrieben.

Darüber hinaus treten noch weitere Faktoren hinzu, die das Eingriffsgewicht erhöhen.

So handelt es sich bei der Quellen-Telekommunikationsüberwachung um eine Maßnahme mit einiger Streubreite. Die Nachrichtendienste erlangen mit der Maßnahme nicht nur Erkenntnisse über die Zielpersonen, sondern zugleich auch über deren Gesprächspartner*innen. Zudem ermöglicht § 3 Abs. 2 Satz 2 G 10 auch die Überwachung nicht verantwortlicher Personen.

Vgl. BVerfGE 113, 348 <383>.

Überdies erhöht die Möglichkeit der Verwendung der erhobenen Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken die Schwere des Eingriffs schon in der Phase der Erhebung. Denn die Daten, die durch die Quellen-Telekommunikationsüberwachung gewonnen werden, können anschließend an weitere Behörden übermittelt (§ 4 Abs. 4 G 10) und als Anlass für Folgemaßnahmen genutzt werden.

Außerdem spielt es für die Eingriffsintensität eine Rolle, dass zur Durchführung der Maßnahme Sicherheitslücken offengehalten werden und über diese staatliche Software auf den Geräten der Betroffenen installiert wird. Es muss nach dem derzeitigen Stand der Technik davon ausgegangen werden, dass diese staatliche Software auch von Dritten genutzt werden könnte, womit unter anderem eine besondere Erpressungsgefahr verbunden ist.

Vgl. BVerfGE 158, 170 <187 Rn. 36 f.>.

Zwar sieht § 11 Abs. 1a Satz 3 und 4 G 10 bestimmte Sicherungsvorgaben vor. So wird die Behörde auf „unerlässliche“ technische Veränderungen beschränkt, die nach dem Ende der Maßnahme „soweit möglich“ rückgängig zu machen sind; die Software ist „nach dem Stand der Technik gegen unbefugte Nutzung zu schützen“. Diese können aber derzeit nicht tatsächlich umgesetzt werden.

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

Zudem ist es für die Quellen-Telekommunikationsüberwachung notwendig, ein informationstechnisches System zu infiltrieren. Damit wird bereits die entscheidende Hürde genommen, um auch auf weitere persönlichkeitsrelevante Informationen zuzugreifen.

Vgl. BVerfGE 120, 274 <308 f.>.

Schließlich schließt das Artikel 10-Gesetz nicht aus, dass die Quellen-Telekommunikationsüberwachung mit anderen Überwachungsmöglichkeiten kombiniert wird. Ein solches Zusammenwirken von Überwachungsmaßnahmen intensiviert den Eingriff zusätzlich.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 284, 287 f.

2. Formelle Verfassungswidrigkeit

§ 11 Abs. 1a Satz 1 G 10 ist bereits formell verfassungswidrig, da die Gesetzgebungskompetenz fehlt, den Landesverfassungsschutzbehörden Befugnisse zu verleihen.

Die Gesetzgebungskompetenz für die nachrichtendienstliche Befugnisse des MAD und des BND ergeben sich aus Art. 73 Abs. 1 Nr. 1 GG. Neben diesen Diensten ermächtigt § 11 Abs. 1a Satz 1 i.V.m. § 3 Abs. 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 jedoch auch die Landesverfassungsschutzbehörden. Für diese Ermächtigung der Landesbehörden fehlt es an einer Gesetzgebungskompetenz des Bundes. Vielmehr liegt diese gem. Art. 70 Abs. 1 GG bei den Ländern.

Eine Gesetzgebungskompetenz des Bundes ergibt sich weder aus Art. 74 Abs. 1 Nr. 1 GG (hierzu **a)**) noch aus Art. 73 Abs. 1 Nr. 1 GG (hierzu **b)**), Art. 73 Abs. 1 Nr. 7 GG (hierzu **c)**), Art. 73 Abs. 1 Nr. 10 b) und c) GG (hierzu **d)**) oder aus ungeschriebenen Gesetzgebungskompetenzen (hierzu **e)**).

a) Art. 74 Abs. 1 Nr. 1 GG nicht einschlägig

In seinem Urteil aus dem Jahr 1970 hielt das angerufene Gericht die Vorschriften des Artikel 10-Gesetzes zur Abwehr verfassungsrechtlicher Bestrebungen im Vorfeld strafprozessualer Ermittlungen von Art. 74 Abs. 1 Nr. 1 GG, das heißt der Kompetenz für „das Strafrecht“, umfasst.

> Vgl. BVerfGE 30, 1 <29>.

Es ist davon auszugehen, dass diese Einschätzung heute nicht länger gilt. Konkret wurde die Kompetenz damals wie folgt begründet:

> Art. 1 § 2 G 10 dient der Abwehr verfassungsfeindlicher Bestrebungen im Vorfeld strafprozessualer Ermittlungen. Die zulässigen Beschränkungsmaßnahmen sind begrenzt auf die Fälle, in denen tatsächliche Anhaltspunkte für den Verdacht bestehen, daß bestimmte strafbare Handlungen geplant, begangen werden oder begangen worden sind. Die Beschränkungsmaßnahmen nach Art. 1 § 2 G 10 dienen also (wenigstens mittelbar) der Verhinderung, Aufklärung und Verfolgung von Straftaten. Die Gesetzgebungskompetenz ist daher insoweit unmittelbar aus Art. 74 Nr. 1 GG zu entnehmen.
>
> BVerfGE 30, 1 <29>.

Eine derart extensive Auslegung von Art. 74 Abs. 1 Nr. 1 weitet „das Strafrecht“ sowohl auf nachrichtendienstliche Maßnahmen als auch auf das Gefahrenabwehrrecht aus. Nachrichtendienstliche Ermittlungen können bereits im Vorfeld von Maßnahmen der Gefahrenabwehrbehörden ergriffen werden. Wenn also die Nähe dieser Maßnahmen zu Straftaten die bundesgesetzliche Kompetenz begründet, dann müsste dies erst recht für Maßnahmen der Gefahrenabwehr gelten. Für diesen Bereich besteht aber Einigkeit, dass es sich um eine Kompetenz der Länder handelt.

> Vgl. BVerfG, Beschluss vom 19. November 2021 – 1 BvR 781/21, Rn. 131; *Uhle*, in: Dürig/Herzog/Scholz, GG, 96. EL November 2021, Art. 70 Rn. 111, vgl. auch *Roggan*, DVBl 2021, 1471 (1472).

Auch entspricht die damalige Einordnung der nachrichtendienstlichen Tätigkeit nicht länger dem heutigen Verständnis. Vielmehr sieht das angerufene Gericht das Tätigkeitsfeld der Nachrichtendienste heute im Bereich der politischen Vorfeldaufklärung und damit eben nicht in der Verhinderung, Aufklärung oder Verfolgung von Straftaten.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 154.; so auch *Roggan*, DVBl 2021, 1471 (1472).

b) Art. 73 Abs. 1 Nr. 1 GG erfasst lediglich BND und MAD

Art. 73 Abs. 1 Nr. 1 GG gibt dem Bund die ausschließliche Gesetzgebungskompetenz über die auswärtigen Angelegenheiten sowie die Verteidigung einschließlich des Zivilschutzes.

Diese verfassungsschriftlichen Vorschriften werden dahingehend ausgelegt, dass damit dem Bund auch die Möglichkeit zusteht, den BND und den MAD mit Befugnissen auszustatten. Die Norm erstreckt sich aber nicht auf die Befugnisse von Landesbehörden.

> *Uhle*, in: Dürig/Herzog/Scholz, GG, 96. EL November 2021, Art. 73 Rn. 41, 45.

c) Art. 73 Abs. 1 Nr. 7 GG nicht einschlägig

Die ausschließliche Kompetenz aus Art. 73 Abs. 1 Nr. 7 GG, die Telekommunikation zu regeln, greift nur für die technische Seite der Telekommunikation, nicht für deren Überwachung. Solche Regelungen sind im Hinblick auf die Regelungskompetenz dem Bereich zuzuordnen, für dessen Zwecke die Überwachung erfolgt.

> BVerfGE 113, 348 <368>; 125, 260 <314>; 130, 151 <193>.

d) Art. 73 Abs. 1 Nr. 10 b) und c) GG nicht einschlägig

Die Gesetzesbegründung beruft sich auf Art. 73 Abs. 1 Nr. 10 GG. Dieser regelt die Bundeskompetenz für die Zusammenarbeit des Bundes und der Länder im Bereich des Verfassungsschutzes (lit. b)) sowie in Bezug auf die Tätigkeiten des BND (lit. c)).

Unter Zusammenarbeit versteht das angerufene Gericht eine auf Dauer angelegte Form der Kooperation, die die laufende gegenseitige Unterrichtung und Auskunftserteilung, die wechselseitige Beratung sowie gegenseitige Unterstützung und Hilfeleistung in den Grenzen der je eigenen Befugnisse umfasst und funktionelle und organisatorische Verbindungen, gemeinschaftliche Einrichtungen und Informationssysteme erlaubt.

> BVerfGE 133, 277 <317 f.>

Eine derartige Zusammenarbeit regelt § 11 Abs. 1a Satz 1 G 10 jedoch nicht. Vielmehr ermächtigt dieser sämtliche der in § 1 Abs. 1 G 10 genannten Behörden, darunter die Landesverfassungsschutzbehörden, eine Quellen-Telekommunikation selbständig und unabhängig von den anderen Nachrichtendiensten durchzuführen. Dies ist nicht von Art. 73 Abs. 1 Nr. 10 b) und lit. c) GG gedeckt.

> So auch *Roggan*, DVBL 2021, 1471 (1472) m.w.N. Vgl. auch *ders.*, G 10, 2. Aufl. 2018, § 3 Rn. 3; *Bergemann*, NVwZ 2015, 1705 (1706); *Bäcker*, DÖV 2011, 840 ff.; *ders.*, DÖV 2012, 560 f.; vgl. *Gröpl,* Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung, 1. Aufl. 1993, S. 114.

Zwar steht es dem Bund auch zu, den Ländern gewisse Mindeststandards für die Aufgabenwahrnehmung vorzugeben. Dies gilt allerdings nur, soweit dies für Sicherstellung einer hinreichenden Effektivität der Zusammenarbeit zwischen Bund und Ländern dient.

> Vgl. BVerwG, Beschluss vom 9. Januar 1995 – 1 B 231.94 1 C 34/94; *Kment*, in: Jarass/Pieroth, GG, 16. Aufl. 2020, Art. 73 Rn. 34; *Bäcker*, in:

Lisken/Denninger, PolR-HdB, B. Die Polizei im Verfassungsgefüge, 7. Aufl. 2021, Rn. 235.

Jedoch müssen auch im Rahmen solcher Mindestvorgaben die Länder weiterhin selbst entscheiden, welche Maßnahmen unter welchen konkreten Voraussetzungen ihre Verfassungsschutzbehörden durchführen dürfen. Es handelt sich schon dem Wortlaut nach um eine Kooperation „des Bundes *und* der Länder" und nicht um eine hierarchisch strukturierte Zusammenarbeit des „Bundes mit den Ländern". Der Kompetenztitel des Art. 73 Abs. 1 Nr. 10 b) und lit. c) GG ändert folglich nichts an der grundsätzlichen Zuständigkeit (Art. 70 Abs. 1 GG) der Länder für den Schutz der inneren Sicherheit.

Vgl. *Uhle*, in: Dürig/Herzog/Scholz, GG, 96. EL November 2021, Art. 73 Rn. 228, 233.

Ein Beispiel für eine derartige Zusammenarbeit, in der der Bund eine einheitliche Regelung schaffen durfte, stellt die Entscheidung *Bestandsdatenauskunft II* dar. In dieser Entscheidung hat das angerufene Gericht auf das „Doppeltürmodell" abgestellt, wonach zwischen der Übermittlungsbefugnis von Daten und der Abrufmöglichkeit zu unterscheiden ist und es beider Befugnisse für einen Datenabruf bedarf. Demnach darf der Bund zwar regeln, dass Unternehmen überhaupt Auskünfte an Behörden erteilen dürfen. Er darf auch die diesbezüglichen Anforderungen festlegen – er öffnet mithin die Tür zur Datenübermittlung. Allerdings steht es den Ländern weiterhin frei, ob sie auch „durch diese Tür gehen" und eine Rechtsgrundlage zum Abruf der Daten schaffen.

Vgl. BVerfGE 130, 151 <184>; 155, 119 <167 f. Rn. 93ff>.

Dieses „Doppeltürmodell" ist jedoch nicht auf die vorliegend gerügten Überwachungsmaßnahmen übertragbar, da den Ländern keine Regelungsmöglichkeit mehr verbleibt. Vielmehr kann sich derzeit jedes LfV unmittelbar auf die Bundesvorschrift des § 11 Abs. 1a G 10 stützen, sodass dem Landesgesetzgeber keinerlei Einflussmöglichkeit verbleibt.

Schließlich kann auch nicht darauf abgestellt werden, dass die Befugnisse nur einen kleinen Ausschnitt der nachrichtendienstlichen Tätigkeiten ausmachen.

> So aber *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, Art. 10-Gesetz, Vor § 1 Rn. 21.

Eine Kompetenzüberschreitung durch den Bund wird nicht dadurch revidiert, dass diese nur kleinen Umfangs ist. Eine solche Argumentation könnte Tür und Tor öffnen, um das Kompetenzgefüge des Grundgesetzes zu unterlaufen. Zudem liegen insbesondere bei den neuen Maßnahmen des § 11 Abs. 1a G 10 äußerst eingriffsintensive Maßnahmen vor. Selbst wenn dem Bund geringfüge Kompetenzübergriffe zu gestatten wären, dann jedenfalls nicht bezüglich Vorschriften von erheblichem Eingriffsgewicht, wie bei der Quellen-Telekommunikationsüberwachung und der beschränkten Online-Durchsuchung.

e) Anderen Kompetenznormen

Auch andere Kompetenznormen sind nicht einschlägig, insbesondere bedarf es keiner Korrektur des obigen Ergebnisses durch Rückgriff auf ungeschriebene Kompetenzen. So besteht bereits kein Bedürfnis, dass der Bund Eingriffsermächtigungen für Landesbehörden zur Quellen-Telekommunikationsüberwachung schafft. Aufbauend auf dem Kompetenzgefüge, nach dem insbesondere die Landesverfassungsschutzbehörden als Länderkompetenz erhalten geblieben sind, ist diesen auch die Entscheidung über Maßnahmen der Vorfeldaufklärung zuzugestehen.

Eine Kompetenz kraft Sachzusammenhangs ist ebenfalls nicht anzunehmen.

> A.A. *Huber*, in: W.-R. Schenke/K. Graulich/J. Ruthig, Sicherheitsrecht des Bundes, Art. 10-Gesetz, Vor § 1 Rn. 21,

Eine derartige Kompetenz würde erfordern, dass eine dem Bund ausdrücklich zugewiesene Materie verständlicherweise nicht geregelt werden kann, ohne dass eine nicht ausdrücklich zugewiesene Materie mitgeregelt wird, mithin

müsste es eine unerlässliche Voraussetzung zur Regelung einer der Bundesgesetzgebung ausdrücklich zugewiesenen Materie sein.

Vgl. BVerfGE 3, 407 <423>.

Davon ist hier gerade nicht auszugehen. Es spricht kein Grund dagegen, die Länder selbst die Befugnisse zum Eingriff in Art. 10 GG regeln zu lassen. Der Bund kann die Zusammenarbeit der Behörden auch ohne derartige Eingriffsbefugnisse regeln.

Schließlich besteht gerade eine ausdrückliche, geschriebene, aber beschränkte Kompetenz des Bundes. Da diese sich nur auf die Zusammenarbeit der Behörden bezieht, darf diese Einschränkung nicht dadurch aufgeweicht werden, dass mittels einer ungeschriebenen Kompetenz doch auch weitere Bereiche des Verfassungsschutzrechts der Länder geregelt werden können.

3. Materielle Verfassungswidrigkeit

Unabhängig von der formellen Verfassungswidrigkeit ist § 11 Abs. 1a Satz 1 G 10 auch materiell nicht mit dem Grundgesetz vereinbar.

Nach der Rechtsprechung des angerufenen Gerichts sind Maßnahmen der Nachrichtendienste insbesondere an der Angemessenheit, also der Verhältnismäßigkeit im engeren Sinne sowie an den Grundsätzen der Bestimmtheit und Normenklarheit zu messen. Hieraus ergeben sich unter anderem Anforderungen an die Eingriffsschwelle, die zu schützenden Rechtsgüter sowie zu Sicherungsvorkehrungen. Die sich dabei konkret ergebenden Anforderungen hängen von der Schwere des Eingriffs ab.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 149 ff.

Aufgrund der erheblichen Eingriffsintensität des § 11 Abs. 1a Satz 1 G 10 ergeben sich hohe Anforderungen an die Vorschrift, die diese jedoch unabhängig vom zugrunde zu legenden Maßstab verfehlt. Es ist davon auszugehen, dass aufgrund des schweren Eingriffsgewichts der Maßnahme dieselben Anforderungen zu stellen sind, die auch für Gefahrenabwehr- und Strafverfolgungsbe-

hörden gelten. Selbst wenn die Maßnahme aber auch nur den hiervon modifizierten Anforderungen an heimliche Überwachungsmaßnahmen unterstellt wird, genügt die Regelung diesen nicht.

a) Voraussetzungen der Maßnahme

(1) Anforderungen an erhebliche Grundrechtseingriffe durch Nachrichtendienste werden nicht erfüllt

§ 11 Abs. 1a Satz 1 i.V.m. § 3 Abs. 1 G 10 wird den verfassungsrechtlichen Anforderungen an besonders schwere Grundrechtseingriffe durch Nachrichtendienste nicht gerecht.

In Bezug auf nachrichtendienstliche Befugnisse besteht das Erfordernis, dass diese an eine hinreichende Eingriffsschwelle geknüpft sein müssen. Dabei gilt der Grundsatz, dass die Eingriffsschwelle die Intensität des Eingriffs zu berücksichtigen hat.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 152 m.w.N.

Zwar gilt grundsätzlich, dass bezüglich der Eingriffsschwelle nicht die gleichen Anforderungen an Nachrichtendienste zu stellen sind, wie an Gefahrenabwehrbehörden. Bei Letzteren droht aufgrund der vorhandenen operativen Anschlussbefugnisse die Gefahr von Folgeeingriffen. Diese Gefahr besteht bei Nachrichtendiensten nicht, sodass im Grundsatz modifizierte Anforderungen an die Eingriffsschwelle zum Tragen kommen.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 159 m.w.N.

Das gilt aber gerade dann nicht, wenn die Grundrechtsbeeinträchtigung durch den Eingriff der Verfassungsschutzbehörde bereits für sich gesehen eine Intensität erlangt, die es unerheblich erscheinen lässt, welche Folgeeingriffe noch durch weitere Verwendungen möglich sind. Das ist dann der Fall, wenn durch die Überwachungsmaßnahme besonders umfangreiche Informationen gewonnen werden und diese eine besonders weitgehende Erfassung der Persönlichkeit zulässt, wie beispielsweise durch eine Online-Durchsuchung.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 166 m.w.N.

Dies zeigt sich bereits daran, dass die Maßnahme eine Intensität erreichen kann, die die Gefahr von Folgemaßnahmen in den Hintergrund treten lässt. Im Rahmen der Quellen-Telekommunikationsüberwachung werden umfangreiche, detaillierte und auch höchst sensible Informationen über die Zielperson gesammelt. Hinzu kommt, dass Überwachungsmaßnahmen im Rahmen der Vorfeldaufklärung davon gekennzeichnet sind, dass diese regelmäßig über Monate oder Jahre aufrechterhalten werden. Zwar begrenzt § 10 Abs. 5 Satz 1 G 10 die Höchstdauer einer einzelnen Anordnung auf drei Monate. Verlängerungen sind aber (jeweils um erneut drei Monate) möglich, solange die Voraussetzungen weiterhin vorliegen, § 10 Abs. 5 Satz 2 G 10. Eine Einschränkung hinsichtlich der so erreichbaren Gesamtdauer besteht nicht.

Vgl. *Zöller,* Nach BVerfG-Urteil: Zeitenwende im Sicherheitsrecht?, LTO vom 29. Juni 2022, abrufbar unter: https://www.lto.de/recht/hintergruende/h/bverfg-sicherheitsrecht-strafprozessrecht-polizeirecht-verfassungsschutz-nachrichtendienste/; *Ogorek*, NJW 2022, 1570 (1571).

Verstärkt wird diese Problematik zudem durch den Umstand, dass von der Quellen-Telekommunikationsüberwachung infolge technischen Fortschritts allgemein und im Bereich des Cloud-Computing besonders – wobei es jedes Mal zu einem Up- und Download kommt, wenn eine Datei in der Cloud bearbeitet wird – mittlerweile auch die Übermittlung von Informationen erfasst werden kann, die über die rein soziale Kommunikation hinausgeht (hierzu ausführlich **D.I.3.a)(2)(d)**).

Als Konsequenz dieser Eingriffsintensität ergibt sich, dass an die Eingriffsvoraussetzungen dieselben Anforderungen zu stellen sind, wie an Überwachungsmaßnahmen durch die Gefahrenabwehrbehörden. Dies bedeutet, dass eine Maßnahme erst ab Vorliegen einer zumindest konkretisierten Gefahr möglich ist.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, 174 f.

Diesen Anforderungen genügt § 3 Abs. 1 G 10 nicht. Vielmehr lässt § 3 Abs. 1 G 10 tatsächliche Anhaltspunkte für einen Verdacht ausreichen. Die Anforderungen an die Tatsachendichte liegen damit deutlich unter der zu fordernden konkretisierten Gefahr.

> Vgl. *Droste,* Handbuch des Verfassungschutzrechts, 1. Aufl. 2007, S. 176 f.; *Gröpl,* Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung, 1. Aufl. 1993, S. 309.

Denn eine konkretisierte Gefahr setzt voraus, dass die Tatsachenbasis sich derart verdichtet hat, dass diese den Schluss auf die Beteiligung bestimmter Personen und auf ein zumindest seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulässt, das mit hinreichender Wahrscheinlich die Verletzung eines Schutzgutes beinhaltet.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 158.

Demgegenüber stellt § 3 Abs. 1 Satz 1 G 10 die Nachrichtendienste vom Erfordernis der konkretisierten Eingriffsschwelle frei, indem „tatsächliche Anhaltspunkte für einen Verdacht“ ohne Anforderung an einen Grad der Sachverhaltskonkretisierung als ausreichend festgelegt werden. Damit hat der Gesetzgeber die Eingriffsschwelle in tatsächlicher Hinsicht bewusst unterhalb der konkretisierten Gefahr angesetzt, um die Nachrichtendienste in die Lage zu versetzen, im Entstehen befindliche Bedrohungsszenarien für die geschützten Rechtsgüter bereits im Vorfeld einer konkretisierten Gefahrenlage erforschen zu können. Die gesetzliche Regelung modifiziert folglich – gemessen am Konkretisierungsgrad – die für einen Eingriff erforderliche Tatsachendichte im Sinne einer Absenkung.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 163.

Über die Tatsachengrundlage hinaus bestehen zusätzliche besondere Anforderungen an derart grundrechtsintensive Eingriffsbefugnisse, die hier ebenfalls keine Beachtung finden. Dazu zählt insbesondere das Erfordernis einer Subsidiaritätsklausel, nach der die Nachrichtendienste nur dann tätig werden können, wenn ein rechtzeitiges Einschreiten der Gefahrenabwehrbehörden

nicht möglich ist (zu den konkreten Anforderungen im Einzelnen siehe **II.2.a)**).

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, 178 f.

(2) Auch modifizierte Anforderungen werden unterschritten

Zudem genügt § 11 Abs. 1a Satz 1 G 10 i.V.m. § 3 Abs. 1 G 10 auch nicht modifizierten Anforderungen. Darunter ist eine Ermächtigungsnorm im Bereich der Nachrichtendienste nur dann verhältnismäßig im engeren Sinne, wenn ein hinreichender verfassungsschutzbezogener Aufklärungsbedarf besteht.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 181.

Dies ist der Fall, wenn hinreichende Anhaltspunkte dafür bestehen, dass eine beobachtungsbedürftige Bestrebung besteht und die ergriffene Aufklärungsmaßnahme auch im Einzelfall geboten ist. Die Annahme einer gegen die Schutzgüter des Verfassungsschutzes gerichteten Bestrebung setzt voraus, dass überhaupt entsprechende Schutzgüter betroffen sind, hinreichende tatsächliche Anhaltspunkte für die Bestrebung bestehen und das Eingriffsgewicht den sich aus der Beobachtungsbedürftigkeit ergebenden Rahmen nicht überschreitet.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 183.

Als Maßstab zur Bestimmung der grundlegenden – für sämtliche ermächtigten Behörden geltende – Eingriffsschwelle für Überwachungsmaßnahmen der Nachrichtendienste kann auf die verfassungsfeindliche Bestrebung zurückgegriffen werden, die einfachgesetzlich in § 1 Abs. 1 Nr. 1 G 10 konkretisiert worden ist.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 184.

Überdies bedarf es Anhaltspunkte, die in Form konkreter und hinreichend verdichteter Umstände als Tatsachenbasis geeignet sind, den Verdacht der verfassungsfeindlichen Bestrebung zu begründen. Je höher dabei die Ein-

griffsintensität der vorzunehmenden Überwachungsmaßnahme wiegt, desto höhere Anforderungen sind auch an deren tatsächliche Grundlage zu stellen.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 188 f.

Dabei sind auch die modifizierten Anforderungen an der Eingriffsintensität der Maßnahme auszurichten. Von besonderem Eingriffsgewicht ist auszugehen, wenn – wie bei der Quellen-Telekommunikationsüberwachung – besonders private Informationen heimlich erlangt werden können, berechtigte Vertraulichkeitserwartungen überwunden werden und eine Überwachungsmaßnahme auch über einen langen Zeitraum aufrechterhalten werden kann.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 191.

Schließlich muss der Gesetzgeber eine hinreichend bestimmte und normenklare Regelung treffen, die dem Eingriffsgewicht der Überwachungsmaßnahme entsprechende Eingriffsschwellen durch Maßgaben zur jeweils erforderlichen Beobachtungsbedürftigkeit festlegt. Es genügt dabei gerade nicht, wenn die Behörde die eingriffsangemessenen Stufen intern den verfassungsrechtlichen Anforderungen anpasst. Vielmehr bedarf es bei grundrechtsintensiven Überwachungsbefugnissen einer hinreichenden Anbindung an Maßgaben des Rechts, die dem demokratischen Gesetzgebungsverfahren entspringen.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 190 ff., 203.

Diesen Anforderungen wird § 11 Abs. 1a Satz 1 G 10 nicht gerecht.

Die Ermächtigungsnorm des § 11 Abs. 1a S.1 G 10 i.V.m. § 3 Abs. 1 G 10 ermächtigt sämtliche Nachrichtendienste gleichermaßen und ist folglich zumindest an der verfassungskonformen Konkretisierung des verfassungsschutzspezifischen Aufklärungsbedarfs im Sinne von § 1 Abs. 1 Nr. 1 G 10 zu messen. Erforderlich ist danach eine hinreichend bestimmte und normenklare Regelung, die im Verdachtsgrad die Eingriffsintensität berücksichtigt (hierzu **(a)**), die eingriffsangemessene Stufen der Beobachtungsbedürftigkeit festlegt (hierzu **(b)**) und nur an Rechtsgüter anknüpft, bei denen es sich um Schutzgüter des Verfassungsschutzes oder vergleichbare besonders bedeutsame Güter von

Verfassungsrang handelt (hierzu **(c)**). Diesen Anforderungen genügt die bestehende Regelung nicht.

Verschärft wird diese Grundrechtsverletzung außerdem durch die Weite des Telekommunikationsbegriffs (hierzu **(d)**).

(a) Eingriffsschwelle ist zu niedrig

Die Regelung des § 11 Abs. 1a Satz 1 G 10 i.V.m. § 3 Abs. 1 G 10 genügt nicht den verfassungsrechtlichen Anforderungen an Maßnahmen mit erheblichem Eingriffsgewicht. Die notwendige Konkretisierungsdichte der Tatsachengrundlage unterschreiten bereits für sich gesehen die verfassungsrechtlichen Vorgaben (hierzu **(i)**). Erst recht gilt dies in Verbindung mit weiteren Tatbestandsvoraussetzungen, die keine Begrenzung darstellen, sondern durch die extensive zeitliche Vorverlagerung der Anknüpfung an strafrechtliche Vorfeld- und Gefährdungsdelikte die Anforderungen nur noch weiter abschwächen (dazu **(ii)**). Unter Berücksichtigung der potenziellen Eingriffsintensität der Quellen-Telekommunikationsüberwachung überschreitet die Konturenlosigkeit der Tatbestandsmerkmale somit den verfassungsrechtlichen Rahmen bezüglich der Anforderungen an die Tatsachengrundlage.

(i) Eingriffsschwelle unterschreitet erforderliche Konkretisierungsdichte der Tatsachenbasis

Die verfassungsrechtlichen Bedenken betreffen zuvorderst die Anforderungen an die Dichte der Tatsachenbasis, ab der eine Überwachungsmaßnahme zulässig ist. Der verfassungsrechtliche Rahmen sieht zwar nicht vor, dass eine Gewissheit darüber besteht, dass Bestrebungen im Sinne der §§ 1 Abs. 1, 3 Abs. 1 G 10 tatsächlich bestehen. Demgegenüber genügt es aber auch nicht, sich von Vermutungen, Spekulationen oder Hypothesen leiten zu lassen, die nicht durch beobachtbare Fakten fundiert sind. Je gewichtiger der durch die Überwachungsmaßnahme vorzunehmende Eingriff ist, desto höhere Anforderungen sind an die tatsächliche Grundlage der Überwachungsmaßnahme zu stellen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 188 f.

§ 3 Abs. 1 G 10 stellt – trotz erheblicher Eingriffstiefe der Quellen-Telekommunikationsüberwachung – keine verschärften Anforderungen an die Tatsachenbasis. Nach § 3 Abs. 1 G 10 reicht es aus, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass eine genannte Straftat zumindest geplant wird bzw. eine Mitgliedschaft in einer in § 3 Abs. 1 Satz 2 G 10 genannten Vereinigung besteht.

Der Wortsinn tatsächlicher Anhaltspunkte besteht darin, dass sich für eine Hypothese ein Anknüpfungspunkt im Objektiven finden lässt, wobei eine irgendwie geartete Konkretisierung noch nicht erfolgt sein muss. Die geringe Konkretisierungsdichte lässt sich auch im systematischen Vergleich mit Parallelregelungen zur Quellen-Telekommunikationsüberwachung wie § 100a Abs. 1 Nr. 1 StPO, § 51 Abs. 1 BKAG, § 54 PolG BW oder § 24 PolDVG Hamburg erkennen. Diese gehen stets über das Erfordernis tatsächlicher Anhaltspunkte hinaus und verengen die Konkretisierungsdichte auf zumindest „bestimmte Tatsachen".

Das angerufene Gericht sieht zwar in der Verwendung des Begriffs „tatsächliche Anhaltspunkte" für sich genommen noch kein Problem. Vielmehr hat es diesen Begriff anknüpfend an die verwaltungsgerichtliche Rechtsprechung dahingehend ausgelegt, dass zwar keine Gewissheit bestehen muss, zugleich aber bloße Vermutungen, Spekulationen oder Hypothesen, die sich nicht auf beobachtbare Fakten stützen können, nicht ausreichen. Anhaltspunkte müssen danach in Form konkreter und hinreichend verdichteter Umstände als Tatsachenbasis geeignet sein, einen Verdacht zu begründen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 188.

Im Rahmen des § 3 Abs. 1 G 10 ist indes zu berücksichtigen, dass dieser nicht tatsächliche Anhaltspunkte für das Bestehen einer Bestrebung fordert, sondern lediglich derartige Anhaltspunkte für einen Verdacht für das Bestehen einer Bestrebung gegeben sein müssen. Setzt man die weite Formulierung tatsächlicher Anhaltspunkte im Rahmen des § 3 Abs. 1 G 10 aber in Verbindung zum Bezugspunkt des „Verdachts", verliert die Eingriffsvoraussetzung so

sehr an Schärfe, dass die verfassungsrechtlichen Anforderungen an den Bestimmtheitsgrad unterschritten werden.

So müssen die tatsächlichen Anhaltspunkte im Rahmen des § 3 Abs. 1 G 10 nicht aufgrund der Absicherung durch Erfahrungssätze ausschlaggebend für die Bestätigung der Hypothese sein. Der Wortlaut lässt vielmehr ausreichen, dass Anhaltspunkte für eine zuvor erdachte prognostische Vermutung bestehen. Die erforderliche Qualität der objektiven Anhaltspunkte reduziert sich damit auf ein absolutes Minimum, sodass nicht ausgeschlossen ist, dass jedwedes sozialadäquates oder auch harmloses Verhalten als Bestätigung für einen bis dahin von Tatsachen losgelösten Verdacht gewertet wird. Die hieraus resultierende besonders hohe Gefahr einer Fehlprognose steht zu den mit einer Überwachungsmaßnahme verbundenen grundrechtlichen Belastungen außer Verhältnis.

Maßgeblicher Zeitpunkt für das Vorliegen der Voraussetzungen ist der Zeitpunkt der Zustimmung der G 10-Kommission. Sowohl der Umfang als auch die Dauer der konkreten Überwachungsmaßnahme sind aber zu diesem Zeitpunkt kaum absehbar und richten sich nach den Erfordernissen im Einzelfall. Art, Umfang und Dauer der Maßnahme sind zwar notwendige Bestandteile der Anordnung (§ 10 Abs. 2 Satz G 10), sodass diese bereits im Antrag auszuführen sind (§ 9 Abs. 3 Satz 2 G 10).

Konkrete Anknüpfungspunkte, nach denen sich Umfang und Dauer der Überwachung zu richten hätten, lassen sich § 11 Abs. 1a G 10 jedoch nicht entnehmen, obwohl diese maßgeblich über das Eingriffsgewicht der Maßnahme bestimmen. Dadurch werden die Anforderungen an die Eingriffsschwelle von den verfassungsrechtlichen Vorgaben entkoppelt. Selbst bei erheblicher Eingriffsintensität einer Überwachungsmaßnahme, bei der die Intensität gerade nicht durch die Gefahr von Folgemaßnahmen geprägt ist, genügte nach § 3 Abs. 1 G 10 weiterhin lediglich ein an tatsächliche Anhaltspunkte anknüpfender Verdacht.

(ii) Weitere Absenkung der Eingriffsschwelle durch Vorfeldbezug

Zusätzlich zu den vorstehenden Mängeln erfährt die Eingriffsschwelle eine weitere Verwässerung durch die Verbindung mit der der Arbeit der Nachrichtendienste immanenten Tätigkeit im Vorfeldbereich und der hier vorgesehenen Anknüpfung an strafrechtliche Vorfeld- und Gefährdungsdelikte.

So knüpft der Eingriffstatbestand nicht an Situationen an, die regelmäßig auf eine auch nur abstrakte Rechtsgutsgefahr schließen lassen, sondern ermöglicht sogar eine Überwachung bereits ab dem Planungsstadium der Anlasstaten. Da das Planungsstadium sich von den frühen Anfängen einer nicht zwingend ausgegorenen Idee bis hin zur konkreten Vorbereitung der Begehung erstreckt, lässt die Regelung gänzlich außer Betracht, dass im frühen Stadium noch erhebliche, sogar mitunter auch unüberwindbare Hürden bestehen. Ein nach Wahrscheinlichkeit der Umsetzung differenzierender Richtwert ist ebenso wenig ersichtlich, wie ein Mindestmaß an Konturierung, den die Deliktsnatur der Bezugstat erlangt haben muss. Angesichts der Uferlosigkeit des Planungsstadiums erfüllt das Merkmal in Verbindung mit den unspezifischen Anforderungen an die Tatsachenbasis nicht die dem Tatbestand zugedachte handlungsbegrenzende Funktion.

> Vgl. BVerfGE 110, 33 <59 f.>; kritisch auch *Huber,* in: Schenke/Graulich/Ruthig, 2. Aufl. 2019, G 10 § 3 Rn. 13; *Hoffmann-Riem,* in: Papier/Münch/Kellermann, Freiheit und Sicherheit – Verfassungspolitik, Grundrechtsschutz, Sicherheitsgesetze, 1. Aufl. 2016, S. 19 (21); *Roggan*, G 10, 2. Online-Aufl. 2018, § 3 Rn. 4.

Überdies verschärft sich diese Problematik dadurch, dass § 3 Abs. 1 G 10 es genügen lässt, dass tatsächliche Anhaltspunkte für den Verdacht vorliegen, dass eine Anlasstat geplant wird und Hinweise auf die Zielrichtung erst durch die Maßnahme erwartet werden.

> Vgl. BR-Drs. 54/01, S. 24.

Im Planungsstadium besteht die Tatsachenbasis im Regelfall nur aus einem durch relativ diffuse Anhaltspunkte für mögliche Straftaten gekennzeichneten, in der Bedeutung der beobachteten Einzelheiten indes häufig nur schwer

fassbaren Geschehen. Erst recht gilt dies dann, wenn die in Bezug genommenen Straftaten durch weit ausgreifende Vorbereitungs- und Gefährdungstatbestände gekennzeichnet sind.

> Vgl. BVerfGE 110, 33 <59>.

Viele der durch § 3 Abs. 1 Nr. 1 bis 8 G 10 in Bezug genommenen Anlassdelikte stellen Gefährdungs- oder nur reine Vorbereitungstatbestände dar und höhlen so die tatbestandlich angedachte Begrenzungswirkung aus. So finden sich zum einen zahlreiche rein abstrakte Gefährdungsdelikte, welche weder eine konkrete Rechtsgutsverletzung noch eine konkrete Gefährdung erfordern. Dies gilt für:

> §§ 80a, 83, 84, 85, 86, 87, 88, 89, 89a–89c, 96, 98, 99, 100, 109f, 129a, 129b, 130, 303a Abs. 3 i.V.m. § 202c, 306a Abs. 1, 316c Abs. 1 StGB, § 95 Abs. 1 Nr. 8 AufenthG, § 13 VStGB.

Eine beträchtliche Anzahl dieser Vorschriften verlagern die Strafbarkeit darüber hinaus erheblich vor, indem diese an Verhaltensweisen anknüpfen, die bereits weit im Voraus einer drohenden Rechtsgutsgefährdung liegen. Dazu zählen insbesondere:

> §§ 83, 87, 89a – c, 96, 98, 99, 100, 109f, 129a, 129b, 303a Abs. 3 i.V.m. § 202c, 13 VStGB.

Die strafrechtliche Rechtsprechung schränkt den Anwendungsbereich von Vorfeld-Tatbeständen wie beispielsweise § 89a Abs. 1 StGB ein, indem hohe Anforderungen an die subjektive Seite der Tatbestandsverwirklichung gestellt werden.

> Vgl. BGH, Urteil vom 27. Oktober 2015 – 3 StR 218/15, Rn. 10.

Dies vermag indes im nachrichtendienstlichen Bereich der präventiven Vorfeldüberwachung nicht zu überzeugen, da sich die konkreten Beweggründe des Handelns selten nachvollziehen lassen.

Die Problematik der Vorfeldverlagerung verdeutlicht sich beispielsweise bei § 3 Abs. 1 Satz 1 Nr. 2 G 10 i.V.m. § 89a Abs. 2a Alt. 2 StGB. Unter Berücksichti-

gung der Erfassung des Planungsstadiums genügen für diesen Fall bereits tatsächliche Anhaltspunkte für den Verdacht einer Planung der Ausreise zum Zwecke des Besuchs eines terroristischen Ausbildungslagers, in dem eine Unterweisung im Schusswaffengebrauch erfolgt. Demgemäß könnten tatsächliche Anhaltspunkte für eine Ausreise zu einem nicht näher definierten Zeitpunkt bereits in der Anmeldung zu einem Sprachkurs oder der Suche nach Bus- oder Flugtickets zu erblicken sein, die den Anlass für eine Quellen-Telekommunikationsüberwachung bieten. Die unbestimmte Weite des Planungsstadiums führt somit zu einer unüberblickbaren Ausdehnung der Überwachungsmöglichkeiten bis in einen Bereich, der weit entfernt von einer auch nur abstrakten Rechtsgutsgefährdung liegt.

Vgl. *Schneider,* ZD 2021, 360 (361).

Ähnlich verhält es sich bei § 3 Abs. 1 Satz 1 Nr. 6 lit. a) G 10 i.V.m. § 129a Abs. 5 Satz 2 StGB, der an das Werben um Mitglieder oder Unterstützer*innen für eine terroristische Vereinigung anknüpfen. Auch hier potenziert sich die – für sich genommen bereits gesetzlich angelegte – Vorverlagerung der strafrechtlichen Anknüpfung durch die Inbezugnahme des Planungsstadiums und die gesteigerte subjektive Komponente des § 129a Abs. 5 Satz 2 StGB. Die Verabredung zu Treffen mit Bekannten droht unter diesen Voraussetzungen ebenso als tatbestandsmäßig erachtet zu werden, wie eine Terminvereinbarung im Copy-Shop, in dem sich beispielsweise Werbematerial herstellen ließe.

Schließlich erlaubt § 3 Abs. 1 G 10 ein Anknüpfen an konkrete Gefährdungstatbestände. Auch hiermit wird ein Eingreifen ermöglicht, obwohl es selbst bei Verwirklichung des Straftatbestandes nicht zu einer Rechtsgutverletzung kommen muss. Hierzu gehören:

> §§ 94, 95, 97a, 97b, 100a, 109e, 109g, 306a Abs. 2, 308 Abs. 1, 315b Abs. 1 i.V.m. 315 Abs. 3 Nr. 1, 315e i.V.m. 315b Abs. 1 i.V.m. 315 Abs. 3 Nr. 1, 316b Abs. 3 StGB.

Der Gesetzgeber hätte durchaus sicherstellen können, dass die Eingriffsschwelle die verfassungsrechtlichen Anforderungen erfüllt. Sei es, indem hö-

here Anforderungen an die Tatsachendichte gestellt würden, sei es, indem den weiten Anforderungen an die Tatsachendichte begrenzende sonstige Merkmale entgegengesetzt würden. In der gegenwärtigen Kombination unterschreitet die Vorschrift jedoch in Anbetracht der Eingriffsintensität die erhöhten verfassungsrechtlichen Anforderungen an den Konkretisierungsgrad der einen Eingriff legitimierenden Voraussetzungen.

Eine vergleichbare Problemlage stellt sich hinsichtlich § 3 Abs. 1 Satz 2 G 10, der ebenfalls weit im Vorfeld konkreter Gefahren eine Überwachung zulässt. Danach genügen tatsächliche Anhaltspunkte für eine Mitgliedschaft in einer Vereinigung, deren Zwecke auf die Begehung von nicht zwingend erheblichen Straftaten gerichtet ist, solange diese eine verfassungsfeindliche Tendenz haben. Der Anlass für eine Überwachungsmaßnahme wird dementsprechend weit vom Bereich der Bedrohung von gewichtigen Rechtsgütern entfernt. Auch dieser Norm fehlt es darüber hinaus an hinreichender Handlungsbegrenzung, indem die Ausrichtung der Vereinigung von tatsächlichen Anhaltpunkten gesetzlich losgelöst bleibt und die Einschätzung deren Gefährdungspotenzial auf reinen Vermutungen beruhen kann. In der Konsequenz birgt dies die Gefahr, dass politisch missliebige Gruppierungen, die beispielsweise dem linksautonomen Spektrum zuzurechnen sind, sich stets dem Vorwurf der verfassungsfeindlichen Ausrichtung ausgesetzt sehen, wenn vergleichbare Gruppen durch Brandanschläge auffällig werden,

Vgl. z.B. VG Berlin, Urteil vom 1. März 2012 – 1 A 398.08.

(b) Keine bestimmte und normenklare Regelung der eingriffsangemessenen Stufen

§ 3 Abs. 1 G 10 enthält keine dem Grundsatz der Bestimmtheit und Normenklarheit genügende Festlegung der eingriffsangemessenen Stufen.

Nach der Rechtsprechung des angerufenen Gerichts ergibt sich die verfassungsrechtlich gebotene Stufenbestimmung aus dem Zusammenspiel der Intensität der Überwachungsmaßnahme sowie der jeweiligen Beobachtungsbedürftigkeit der (vermeintlichen) verfassungsfeindlichen Bestrebung.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 190.

Die Quellen-Telekommunikationsüberwachung stellt einen schwerwiegenden Eingriff dar (hierzu **1.**), sodass eine Konkretisierung der Beobachtungsbedürftigkeit der Bestrebung vorzusehen ist.

Diese bemisst sich vor allem nach der Intensität der Bedrohung von § 1 Abs. 1 Nr. 1 G 10 geschützten Güter. Für eine gesteigerte Beobachtungsbedürftigkeit sprechen neben einer verdichteten Tatsachenbasis als Entscheidungsgrundlage, die potenzielle Gewaltanwendung sowie Größe, Abschottungsgrad und gesellschaftlicher Einfluss der verfassungsfeindlichen Bestrebung. Dagegen kann die Beobachtungsbedürftigkeit sinken, wenn sich die Bestrebung durch Arbeit mit legalen Mitteln auszeichnet, ohne auf eine besonders schwere Straftat ausgerichtet zu sein oder sich auch nach Beginn der Überwachung die Tatsachenbasis für den Verdacht der Bedrohung der Schutzgüter nicht verdichtet.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 193 ff.

Der Gesetzgeber ist nach der Rechtsprechung des angerufenen Gerichts dazu verpflichtet, diese unterschiedlichen Ausformungen der Beobachtungsbedürftigkeit in einer gesetzlichen Regelung festzuhalten. Obgleich die handelnde Behörde aufgrund ihrer Grundrechtsbindung zur verhältnismäßigen Ausübung ihrer Befugnisse verpflichtet ist, kann die Konkretisierung der verfassungsrechtlichen Anforderungen gerade im Bereich heimlicher Überwachungsmaßnahmen dieser nicht vollständig überantwortet werden. Denn im nachrichtendienstlichen Bereich kann nur eine ausreichend spezifische gesetzliche Regelung die Defizite kompensieren, die sich wegen der verengten Rechtsschutzmöglichkeiten sowie der eingeschränkten Normkonkretisierung im Wechselspiel zwischen Anwendungspraxis und unabhängiger Kontrolle im Recht der nachrichtendienstlichen Überwachungsbefugnisse ergeben.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 200.

Zwar erscheint bei Überwachungsmaßnahmen nach dem Artikel 10-Gesetz eine schrittweise Konkretisierung der oben ausgeführten unspezifischen Eingriffsvoraussetzungen durch die Kontrollbefugnis der G 10-Kommission

denkbar. Dies kann jedoch nicht darüber hinweghelfen, dass es gemessen an der Intensität der im Raum stehenden Grundrechtseingriffe von Verfassungs wegen einer hinreichenden Anbindung an Maßgaben des Rechts bedarf, die dem demokratischen Gesetzgebungsverfahren entspringen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 203.

Dementsprechend verfehlt § 3 Abs. 1 G 10 die verfassungsrechtlichen Anforderungen, indem die Erheblichkeit einer verfassungsfeindlichen Bestrebung tatbestandlich nicht in Beziehung zur Intensität der konkreten Quellen-Telekommunikationsüberwachung gesetzt wird. Vielmehr beschränkt sich die Ermächtigungsnorm darauf, dass das bloße Bestehen der verfassungsfeindlichen Bestrebung für eine Überwachungsmaßnahme ausreicht. Die vom angerufenen Gericht geforderten Kriterien, die eine Bemessung der Beobachtungsbedürftigkeit der Bestrebung festlegen, fehlen dagegen gänzlich.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 202.

(c) Unzureichende Einschränkung der geschützten Rechtsgüter

Darüber hinaus überschreiten auch die durch § 3 Abs. 1 G 10 in Bezug genommenen Straftaten den verfassungsrechtlich erlaubten Rahmen.

Die grundlegende Eingriffsschwelle, die für alle Nachrichtendienste Anwendung findet, ergibt sich aus dem Erfordernis der verfassungsfeindlichen Bestrebung. Dies setzt ein Vorgehen voraus, welches gegen die Schutzgüter der Nachrichtendienste im Sinne des § 1 Abs. 1 Nr. 1 G 10 gerichtet ist.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 184.

Die Aufgabe der Nachrichtendienste besteht danach in dem legitimen Zweck, drohende Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes abzuwehren.

Bei § 3 Abs. 1 G 10 besteht jedoch die Besonderheit, dass anhand eines Straftatenkatalogs näher bestimmt wird, wann ein Eingreifen möglich ist. Danach soll die Begehung oder Planung dieser Straftaten indizieren, dass das Verhal-

ten der zu überwachenden Personen eine gewisse politische Relevanz besitzt und die Bereitschaft besteht, verfassungsfeindliche Ziele auch mit rechtswidrigen Mitteln zu begehen.

> *Roggan*, G 10, 2. Online-Aufl. 2018, § 3 Rn. 4; *Poscher/Rusteberg*, KJ 2014, 57 (67); *Wollweber,* in ZRP 2001, 213 (213 f.).

Dabei entfernt sich die konkrete Ausformung der Regelung aber weit von den Zielen des Schutzes der freiheitlichen demokratischen Grundordnung sowie des Bestandes des Bundes oder eines Landes. Vielmehr ermöglicht die Regelung auch ein Eingreifen, das – zumindest angesichts des intensiven Eingriffs des § 11 Abs. 1a Satz 1 G 10 – nicht mehr als verfassungsrechtlich angemessen angesehen werden kann. Verfassungsfeindliche Agitation erlangt nämlich erst dann ihren Bestrebungscharakter, wenn diese über das bloße Vorhandensein einer politischen Meinung hinausgeht, auf die Durchsetzung eines politischen Ziels unter Beeinträchtigung eines der Elemente der freiheitlichen demokratischen Grundordnung ausgerichtet ist und vor allen Dingen objektiv geeignet ist, über kurz oder lang politische Wirkungen zu entfalten.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 185 f.

Das strafrechtlich relevante Verhalten muss damit erstens eine solche Erheblichkeit erreicht haben, dass diesem unter Bedrohung besonders gewichtiger Rechtsgüter die Eignung zur Entfaltung politischer Wirkung innewohnt. Zweitens darf – wie sich aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne ergibt – das vom Gesetzgeber bestimmte Gewicht der Anlasstat, das vor allem im Regelstrafrahmen Niederschlag findet, nicht außer Verhältnis zu dem mit der Quellen-Telekommunikationsüberwachung einhergehenden Grundrechtseingriff stehen.

Sowohl § 3 Abs. 1 Satz 1 G 10 als auch § 3 Abs. 1 Satz 2 G 10 verfehlen diese Anforderungen.

So enthält § 3 Abs. 1 Satz 1 G 10 Delikte, die einen Bezug zur verfassungsfeindlichen Bestrebung nicht erkennen lassen. Des Weiteren verweist die Regelung teilweise auf Delikte im Bereich mittlerer und Bagatellkriminalität, deren

Handlungsunwert nicht mit der Eingriffstiefe korrespondiert. § 3 Abs. 1 Satz 2 G 10 löst die grundrechtliche Bindung an einen erhöhten Unrechtsgehalt des kriminalisierten Verhaltens sogar vollständig.

Einige der in § 3 Abs. 1 Satz 1 G 10 aufgezählten Delikte schützen nicht ausschließlich die genannten, besonders bedeutsamen, sondern auch sonstige Schutzgüter, wie beispielsweise das Eigentum oder die Sicherheit des zivilen Luft- und Seeverkehrs. Dies gilt für:

> §§ 308 Abs. 1 (Eigentum), 316c Abs. 1 StGB (Sicherheit des zivilen Luft- und Seeverkehrs)

Zahlreiche weitere Delikte erfassen sogar ausschließlich sonstige Rechtsgüter. Zu den geschützten Rechtsgütern zählen hier beispielweise dasjenige des persönlichen Lebens- und Geheimbereichs oder das Universalrechtsgut der Verkehrssicherheit, die allenfalls als Rechtsreflex die besonders bedeutsamen Rechtsgüter mittelbar in den Schutzbereich mit einbeziehen:

> §§ 202a, 202b, 303a, 303a Abs. 3 i.V.m. 202c, 303b Abs. 1 (Schutz des persönlichen Lebens- und Geheimbereichs), 315b Abs. 1 i.V.m. § 315 Abs. 3 Nr. 1, 315e i.V.m. 315b Abs. 1 i.V.m. § 315 Abs. 3 Nr. 1 StGB (Sicherheit des Straßen- und Schienenverkehrs)

Des Weiteren verweist § 3 Abs. 1 Satz 1 G 10 teilweise auf Delikte im Bereich mittlerer und Bagatellkriminalität, deren Handlungsunwert nicht mit der Eingriffstiefe korrespondiert und somit die Grenzen der Angemessenheit überschreitet. In Bezug auf die Quellen-Telekommunikationsüberwachung überwiegt die Eingriffsintensität hier bei weitem die Schwere der Anlasstat.

> So auch *Bäcker,* in: Dietrich et. al, Nachrichtendienste im demokratischen Rechtsstaat – Kontrolle – Rechtsschutz – Kooperationen, 1. Aufl. 2018, S. 137 (146); *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste, Verfassungsblog vom 6. Juli 2021, abrufbar unter https://verfassungsblog.de/staatstrojaner-nachrichtendienste/. *Roggan*, G 10, 2. Online-Aufl. 2018, § 3 Rn. 10.

So ermöglicht die Vorschrift in Verbindung mit § 11 Abs. 1a Satz 1 G 10 den Einsatz von Quellen-Telekommunikationsüberwachung bei Anhaltspunkten, dass Delikte geplant werden, deren Strafrahmen mit lediglich bis zu einem Jahr Freiheitsstrafe bestraft wird, namentlich:

> § 20 Abs. 1 Nr. 1 – 4 VereinsG, § 95 Abs. 1 Nr. 8 AufenthG

Dies trifft auch zu hinsichtlich derjenigen Straftaten zu, die wie

> §§ 202b, 303a Abs. 1, 303a Abs. 3 i.V.m. § 202c StGB eine Höchstfreiheitsstrafe von zwei Jahren und
>
> §§ 86 Abs. 1, 2, 130 Abs. 2, 4, 202a, 303b Abs. 1 StGB eine Höchstfreiheitsstrafe von drei Jahren

aufweisen.

Auch § 3 Abs. 1 Satz 2 G 10 erfüllt die verfassungsrechtlichen Anforderungen nicht, vielmehr löst die Vorschrift die grundrechtliche Bindung an einen erhöhten Unrechtsgehalt des kriminalisierten Verhaltens sogar vollständig.

§ 3 Abs. 1 Satz 2 G 10 fordert lediglich tatsächliche Anhaltspunkte für den Verdacht, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, die in der Norm umschriebenen Straftaten zu begehen. Eine Differenzierung nach Bedeutung der Zielperson im Personengefüge des Vereins erfolgt nicht, sodass in Verbindung mit dem bloßen Erfordernis des Verdachts der Mitgliedschaft eine Ausweitung auf sämtliche mit Vereinsmitgliedern in zwischenmenschlichem Kontakt stehenden Personen droht. Zudem findet keine Beschränkung auf bestimmte Delikte statt, sodass der Verdacht der Mitgliedschaft in einer Vereinigung genügen kann, die zwar mit verfassungsfeindlicher Intention agiert, von der aber lediglich Bagatelldelikte zu erwarten sind. So ist es denkbar, dass Vereinigungen, die darauf ausgerichtet sind, politischen Protest in aktivistischer, dem illegalen Bereich zuzuordnender Form auszuüben, eine verfassungsfeindliche Intention unterstellt werden und damit ein Anlass zur Überwachung ihrer Mitglieder besteht. Mögliche Protestformen könnten in diesem Rahmen beispielsweise darin be-

stehen, dass Einrichtungen des Bundes unter Verstoß gegen § 123 Abs. 1 StGB besetzt oder unter Verstoß gegen § 303 Abs. 1 StGB beschädigt werden. Mit der vollkommenen Loslösung der Ausrichtung der Vereinigung von der Bindung an besonders erhebliche Straftaten schafft der Gesetzgeber die Möglichkeit von unverhältnismäßigen Grundrechtseingriffen.

Diese Defizite werden nicht durch die Regelung des § 1 Abs. 1 G 10 kompensiert, der die Zwecke der nachrichtendienstlichen Aktivität nennt. § 3 Abs. 1 G 10 konkretisiert gerade die hierin genannten Zwecke in Bezug auf Eingriffsermächtigungen.

Nach der Rechtsprechung des angerufenen Gerichts sind Eingriffsermächtigungen zudem auch in ihrer Gesamtheit zu bewerten. Dementsprechend können selbst Regelungen, die an sich (gerade) noch verfassungsrechtlich zulässige Eingriffsschwellen und geschützte Rechtsgüter enthalten, in ihrer Kombination als unangemessen erscheinen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 284, 287 f.

Im Rahmen des § 11 Abs. 1a Satz 1 G 10 intensiviert das Zusammenwirken der zu geringen Eingriffsschwellen mit dem zu weit ausgestalteten Katalog an Anlasstaten die Grundrechtsverletzung.

(d) Ausweitung des Anwendungsbereichs durch weiten Begriff von „Kommunikation“

Die Grundrechtsverletzung wird zusätzlich dadurch intensiviert, dass der Begriff der Telekommunikation, der auch für § 11 Abs. 1a Satz 1 G 10 von zentraler Bedeutung ist, mittlerweile eine erhebliche Ausweitung erfahren hat. Er geht über das klassische Telefonat weit hinaus. Dies schließt unser Surf-Verhalten, die Übermittlung von Dateien (Dokumente, Fotos, Videos) aber auch Cloud-Computing mit ein und ermöglicht so eine Aggregierung und Verknüpfung von Daten bis hin zur Rekonstruktion eines persönlichen Verhaltensprofils.

Vgl. *Rossi*, in: Papier/Münch/Kellermann, Freiheit und Sicherheit – Verfassungspolitik, Grundrechtsschutz, Sicherheitsgesetze, 1. Aufl. 2016, S. 125 (142 ff.); *Masing*, in: Dietrich et. al, Nachrichtendienste im demokratischen Rechtsstaat – Kontrolle – Rechtsschutz – Kooperationen, 1. Aufl. 2018, S. 1 (5).

Für die vergleichbare Vorschrift im Bereich der Strafverfolgung (§ 100a StPO) geht die herrschende Meinung davon aus, dass der Begriff der Telekommunikation, angelehnt an § 3 Nr. 59, 60 Telekommunikationsgesetz (TKG), weit auszulegen ist. Danach kommt es beim Begriff Telekommunikation nicht darauf an, ob eine menschliche Interaktion zugrunde liegt. Vielmehr ist auch der reine Austausch von Daten erfasst. Dies schließt das Surfen, den Up- und Download und das Cloud-Computing mit ein.

Vgl. BGH, Beschluss vom 14. Oktober 2020 – 5 StR 229/19.

Es ist nicht ersichtlich, weshalb sich im Rahmen der nachrichtendienstlichen Beobachtung strengere Maßstäbe ergeben sollten. Zwar ist die Weite dieses Begriffs äußerst problematisch. Jedoch bestehen gegenüber den Gefahrenabwehr- und Strafverfolgungsbehörden keine derartigen Unterschiede, die gerade bei den Nachrichtendiensten eine einschränkende Auslegung nahelegen würden. So arbeiten die Nachrichtendienste in der Vorfeldaufklärung, sodass gerade bei diesen ein weiter Telekommunikationsbegriff diese Aufgabe zu fördern vermag. Zudem fehlt es bei den Nachrichtendiensten gerade an operativen Anschlussbefugnissen, sodass Eingriffe durch diese grundsätzlich von einer geringeren Intensität geprägt sind.

Das führt zu einer erheblichen Ausweitung der Überwachungsbefugnisse. So ermöglicht bereits das Surfverhalten erhebliche Erkenntnisse über Personen. Durch den Up- und Download und Cloud-Computing werden zudem Dateien, die zunächst nicht für eine andere Person gedacht waren, zur Kommunikationsdaten, beispielsweise, wenn eine Datei zu Sicherungszwecken hoch- oder runtergeladen wird. Gerade beim Cloud-Computing kommt es immer dann zu einem derartigen Up- und Download, wenn eine Datei in der Cloud bearbeitet

wird. Wird ein neues System verwendet, werden auch viele ältere Dateien mit dem neuen System synchronisiert und damit erneut kommuniziert.

Dadurch verliert auch die Einschränkung des § 11 Abs. 1a Satz 1 G 10, dass es sich um Kommunikation handeln muss, die nach dem Zeitpunkt der Anordnung übertragen worden ist, erheblich an Bedeutung. Auch eine Datei, die vor Jahren erstellt wurde, kann durch das Cloud-Computing regelmäßig erneut hoch- oder runtergeladen – und damit kommuniziert – werden. Damit wird der Zugriff auf diese Daten ermöglicht.

Das angerufene Gericht hat sich in einem Nichtannahmebeschluss mit der grundsätzlichen Reichweite des Telekommunikationsbegriffs in Bezug auf die Befugnis zur Quellen-Telekommunikationsüberwachung im Rahmen der Strafverfolgung auseinandergesetzt. Danach ist auch eine weite Auslegung des Telekommunikationsbegriffs verfassungsrechtlich unbedenklich, soweit diese Kommunikation willensgesteuert stattfindet.

BVerfG[K], Beschluss vom 6. Juli 2016 – 2 BvR 1454/13, Rn. 29 ff.

Damit ist zunächst davon auszugehen, dass Surfen, aber auch der manuelle Up- oder Download vom Telekommunikationsbegriff umfasst sind. Bereits aus diesem Umstand ergibt sich eine erhebliche Reichweite der Quellen-Telekommunikationsüberwachung.

Zudem erfüllt auch das Cloud-Computing diese Vorgaben. Auch dieses ist zumindest zu Beginn ebenfalls von den Nutzer*innen willensgesteuert gestartet worden. Danach folgt die weitere Kommunikation zwar automatisiert, dies ist jedoch von den Nutzer*innen so gewollt und erfolgt in dem Bewusstsein, dass eine Cloud verwendet wird.

Selbst wenn mit der Mindermeinung davon ausgegangen werden sollte, dass der Begriff der Kommunikation ein Element der sozialen Interaktion oder vergleichbare Einschränkungen enthalten muss, ergibt sich selbst daraus keine weitreichende Einschränkung des Telekommunikationsbegriffs.

Vgl. zu dieser restriktiven Auslegung z.B. *Hiéramente*, StraFO 2013, 96 (99), *ders./Fenina*, StraFo 2015, 365 (369 ff.), *Roggan*, StV 2017, 821 (823); ; *Schneider*, Fernmeldegeheimnis und Fernmeldeaufklärung, 1. Aufl. 2020, S. 60 ff.

Denn im Rahmen der technologischen Entwicklung verwischen die Grenzen zwischen sozialer und technischer Interaktion zunehmend. Als Beispiel können hier die Anwendungen auf einem Mobiltelefon herangezogen werden, die mittlerweile fast alle ein Element der sozialen Interaktion beinhalten. Neben Messenger-Diensten liegt auch bei sozialen Netzwerken und Dating-Apps der Kern der Anwendungen im Bereich der sozialen Interaktion. Bereits die Überwachung allein dieser Anwendungen ermöglicht erhebliche Aufschlüsse über die Persönlichkeit von Nutzer*innen. Auch darüber hinaus setzen mehr und mehr Anwendungen auf Komponenten sozialer Interaktion. So haben selbst Spiele, Fitnessprogramme (beispielsweise *Strava*) und Lernanwendungen (beispielsweise *Duolingo*) einen ausgeprägten sozialen Interaktionsaspekt. Andere Apps erlauben das Versenden von Daten an andere Personen, beispielsweise Anwendungen zur Aufzeichnung von Menstruationszyklen und auch die Health-App von Apple hat ein prominentes „Teilen"-Feature. Mit diesen Anwendungen werden also auch höchst-sensible Daten mit anderen im Rahmen einer sozialen Interaktion geteilt.

Die Weite des Telekommunikationsbegriff intensiviert den – bereits bei einem engen Begriffsverständnis vorliegenden – Verfassungsverstoß. Unter diesem Verständnis ermöglicht die Norm die Erfassung einer großen Zahl an Informationen, die klassisch nicht von der Telekommunikationsüberwachung erfasst werden konnte, unter den bereits allgemein vorliegenden verfassungsrechtlichen Mängeln der Vorschrift.

Jedenfalls aber führt die technologische Fortentwicklung dazu, dass die Vorschrift nicht den Bestimmtheitsanforderungen entspricht. Vor dem Hintergrund der Eingriffsintensität der Maßnahme ist der Gesetzgeber verpflichtet, anhand von Kriterien aufzuzeigen, welche Formen von Telekommunikation von § 11 Abs. 1a Satz 1 G 10 erfasst sein sollen.

b) Unzureichender Schutz des Kernbereichs privater Lebensgestaltung § 3a G 10

Das angerufene Gericht hat zuletzt in seiner Entscheidung zum *Bayerischen Verfassungsschutzgesetz* ausgeführt, welche Anforderungen an den Schutz des Kernbereichs zu stellen sind. Das Gericht nimmt dabei keine Differenzierung zwischen dem Gefahrenabwehrrecht und dem Recht der Nachrichtendienste vor. Der Kernbereichsschutz ist zudem strikt und darf nicht durch eine Abwägung mit Sicherheitsinteressen relativiert werden. Konkret umfasst er zwei Ausformungen.

Erstens sind bereits auf der Ebene der Datenerhebung Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen. Zweitens sind auf der Ebene der nachgelagerten Auswertung und Verwertung die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren.

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 277 m.w.N.

Wenn eine Aussonderung der kernbereichsrelevanten Daten nicht vor oder bei der Erhebung erfolgen kann, bedarf es einer Sichtung durch eine unabhängige Stelle, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung durch den Nachrichtendienst herausfiltert.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 286 m.w.N.

Diese Anforderungen erfüllen die Regelungen des Kernbereichsschutzes im Artikel 10-Gesetz nicht.

Nach § 3a Abs. 1 Satz 2 und 3 G 10, sind die Informationen zunächst nur aufzuzeichnen und einem Mitglied der G 10-Kommission vorzulegen, wenn Zweifel darüber bestehen, ob kernbereichsrelevante Informationen betroffen sind.

Hierbei besteht jedoch eine Ausnahme bei Gefahr im Verzug, sodass die Sichtung dann durch die Behörde selbst erfolgt. Voraussetzung ist lediglich, dass

ein Bediensteter, der die Befähigung zum Richteramt hat, die Sichtung beaufsichtigt (§ 3a Abs. 2 Satz 1 G 10). Diese Ausnahme widerspricht den verfassungsrechtlichen Anforderungen. So ist zunächst fraglich, inwiefern es bei nachrichtendienstlicher Überwachung und damit in der Vorfeldaufklärung überhaupt einer Ausnahme für Gefahr im Verzug bedürfte. Vielmehr liegt nahe, bei Gefahr im Verzug Rückgriff auf die Gefahrenabwehrbehörden zu nehmen.

Selbst wenn aber ein derartiges Bedürfnis bestünde, müssten auch hier möglichst hohe Anforderungen zur Sicherung des Kernbereichsschutzes getroffen werden. Dementsprechend reicht es nicht aus, dass die Sichtung unter Aufsicht eines Bediensteten mit Befähigung zum Richteramt erfolgt. Vielmehr ist zu fordern, dass dieser selbst die Sichtung vornimmt. Es besteht kein Bedürfnis, dass weitere Personen in die Sichtung eingebunden werden müssen, die dann potenziell kernbereichsrelevante Informationen in Erfahrung bringen. Für die Erkenntnis, ob eine kernbereichsrelevante Information vorliegt, bedarf es keiner weiteren Kenntnisse beispielsweise über den Überwachungsanlass, da eine Abwägung zwischen diesem und dem Kernbereichsschutz gerade nicht stattzufinden hat. Eine Sichtung durch den*die zum Richteramt befähigte*n Beschäftigte*n alleine wäre mithin vollkommen ausreichend und ist daher als Mindestmaß verfassungsrechtlich zu fordern.

Darüber hinaus ist problematisch, dass lediglich solche Aufzeichnungen einer Kontrolle vorzulegen sind, bei denen Zweifel hinsichtlich bestehender kernbereichsrelevanter Informationen bestehen. Die Quellen-Telekommunikationsüberwachung findet in einem Bereich statt, der aufgrund der Überwachung auch von persönlichen Gesprächen generell eine Nähe zu kernbereichsrelevanten Themen aufzeigt.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 276.

Zum Ausgleich des Umstandes, dass dementsprechend nicht bereits auf Erhebungsebene vollkommen ausgeschlossen werden kann, dass kernbereichsrelevante Informationen erfasst werden, bedarf es jedoch einer umfassenden externen Kontrolle der erfassten Daten.

Vgl. zur Online-Durchsuchung BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 282 f., 315.

Eine solche liegt hier aber nicht vor. So werden lediglich automatische Aufzeichnungen nach § 3a Abs. 1 Satz 4 G 10 einer externen Kontrolle zugeführt. Dies ist unzureichend, da nicht nur bei diesen kernbereichsrelevante Informationen betroffen sein können. Dies ist auch bei der Quellen-Telekommunikationsüberwachung möglich, wie der Vergleich mit der akustischen Wohnraumüberwachung zeigt, bei der das angerufene Gericht gerade eine solche externe Kontrolle aller Daten gefordert hat.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 306.

c) Verfahrenssicherungen weisen Lücken auf

Nach der Rechtsprechung des angerufenen Gerichts ergeben sich aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne zudem prozedurale Anforderungen an die Ausgestaltung von Überwachungsbefugnissen. Dazu gehören unter anderem eine unabhängige Vorabkontrolle, Benachrichtigungspflichten und Auskunftsrechte. Dabei können besondere Geheimhaltungsbedürfnisse Modifikationen begründen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 289.

Zwar enthält das Artikel 10-Gesetz grundsätzlich die geforderten Verfahrenssicherungen. Jedoch sieht das Gesetz Ausnahmevorschriften vor, die zu gravierenden Lücken der jeweiligen Sicherungsvorschriften führen.

(1) Unzulässige Erstreckung auf weitere Kennungen § 11 Abs. 1b G 10

Nach § 11 Abs. 1b Satz 1 G 10 darf eine zuvor angeordnete Maßnahme auch auf Kennungen von Telekommunikationsanschlüssen erstreckt werden, die erst nach der Anordnung bekannt werden. Die Vorschrift gilt nicht für Maßnahmen gegen nicht verantwortliche Personen (§ 11 Abs. 1b Satz 2 G 10).

Konsequenz der Vorschrift ist, dass für derartige Fälle zunächst die Antragspflicht (§ 9 G 10) entfällt und auch keine neue Anordnung (§ 10 G 10) ergeht. Außerdem entfällt die Verpflichtung, vor Vollzug der Maßnahme die Zustimmung der G 10-Kommission abzuwarten, da sich dieses Erfordernis nur auf angeordnete Maßnahmen bezieht (§ 15 Abs. 6 Satz 1 und 2 G 10). Damit werden fundamentale Verfahrensvorschriften ausgehebelt. Die Notwendigkeit der Nennung einer Kennung in Antrag und Anordnung dient gerade auch der Kontrolle durch die G 10-Kommission.

Vgl. BT-Drs. 14/5655.

Besonders problematisch wirkt sich aus, dass die Vorschrift nicht auf Anschlusskennungen der gleichen Art begrenzt ist. Daher ist es möglich, dass bei einer Anordnung in Bezug auf eine Rufnummer eine Anschlussmaßnahme bezüglich einer informationstechnischen Kennung ergriffen wird und damit auch beispielsweise die Kommunikation über Apps oder andere Formen von Telekommunikation überwacht werden. Im Ergebnis könnte nach der Anordnung einer Einzelmaßnahme damit faktisch die gesamte Kommunikation einer Person überwacht werden, ohne dass es hinreichende Sicherungsmechanismen gäbe.

Siehe auch *Roggan*, DVBl 2021, 1471 (1475).

Als Grund für diese Möglichkeit verweist die Gesetzesbegründung auf den Evaluierungsbericht des Instituts für Gesetzesfolgenabschätzung und Evaluation zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen.

Vgl. BR-Drs. 674/20.

Danach besteht das Problem im häufigen Wechsel von SIM-Karten oder Mobiltelefonen.

> Institut für Gesetzesfolgenabschätzung und Evaluation, Evaluation nach Artikel 5 Gesetz zur Verlängerung der Befristung von Vorschrif-

ten nach den Terrorismusbekämpfungsgesetzen vom 3. Dezember 2015, S. 143.

Dies kann jedoch die sehr weitreichende Einschränkung des § 11 Abs. 1b G 10 nicht rechtfertigen.

Zunächst ist den Besonderheiten moderner Kommunikation bereits durch Modalitäten der Anordnung selbst begegnet worden. So kann gem. § 10 Abs. 3 Satz 2 G 10 sowohl an die Kennung eines Anschlusses (beispielsweise eine Rufnummer) als auch an die Kennung eines Endgerätes angeknüpft werden. Dadurch wird gerade verhindert, dass durch einfachen Austausch entweder der SIM-Karte oder des Gerätes eine Überwachungsmaßnahme vereitelt werden kann.

BT-Dr 16/509, S. 11*; Roggan*, G 10, 2. Online-Aufl. 2018, § 10 Rn. 10; *Huber*, in: Erbs/Kohlhaas, G 10, 239. EL Dezember 2021, § 10 Rn. 9; *Huber*, NVwZ 2009, 1321 (1327).

Zwar besteht die Gefahr, dass beides ausgetauscht wird. Aber auch hier ist nicht ersichtlich, weshalb derart weitgehende Einschränkungen der Verfahrensvorschriften in Kauf genommen werden müssten. Für derartige Fälle, in denen eine Anordnung besonders eilig ist, besteht aber gerade die Sonderregelung des § 15a G 10, wonach Maßnahmen bei Gefahr im Verzug bereits vor der Zustimmung durch die G 10-Kommission durchgeführt werden können. Deren Vorsitzende*r muss die Maßnahme dann aber im Nachhinein bestätigen. Damit besteht ein System das – leider nur im Grundsatz (siehe **(3)**) – den Bedürfnissen bei Gefahr im Verzug gerecht wird, zugleich aber eine prozedurale Absicherung vorsieht.

Sofern es bei der Möglichkeit nach § 11 Abs. 1b G 10 lediglich darum geht, prozedurale Vereinfachungen einzuführen, da bei dem neuen Antrag und der neuen Anordnung lediglich eine neue Kennung besteht, so ist nicht ersichtlich, dass hiermit die Regelung des § 11 Abs. 1b G 10 gerechtfertigt werden könnte. Zunächst schützen die Verfahrensrechte die Grundrechte der betroffenen Personen. Die Aufnahme auch der Kennung in Anordnung und Antrag stellt gera-

de sicher, dass nicht nur die Person, sondern auch die Kennung identifiziert wurde und die Maßnahme damit keine Dritten treffen kann. Damit unterliegt eben auch die Kennung der Kontrolle durch die G 10-Kommission.

Darüber hinaus ist bereits fraglich, ob es bei derartigen Anschlussmaßnahmen tatsächlich zu prozeduralen Hürden kommt. Vielmehr wird auch der G 10-Kommission bekannt sein, dass eine Anschlussmaßnahme bezüglich einer neuen Kennung vorliegt. Dies kann auch in den Antrag mit aufgenommen werden. Dem Evaluierungsbericht lassen sich keine genauen Angaben dazu entnehmen, ob bzw. zu welchem Grad es zu derartigen Verzögerungen gekommen ist.

Selbst wenn aber derartige Verzögerungen tatsächlich ein Problem in der Praxis darstellten, ließe sich dem durch ein vereinfachtes Verfahren begegnen. Die vollkommene Ausschaltung der Verfahrenssicherung geht zu weit.

Sofern hier eine restriktive verfassungskonforme Interpretation anzudenken ist, würde eine solche wohl gegen den Willen des Gesetzgebers verstoßen. Die Umgehungsmöglichkeiten, die durch den Austausch von SIM-Karten bestehen, bestehen in gleicher Weise durch den Wechsel von einem Messenger-Dienst zum nächsten oder von Telefonie auf Messenger-Dienste. Jedenfalls würde die Vorschrift dann aber die Grenzen der Bestimmtheit überschreiten. Gerade im Bereich der Einschränkungen von Verfahrenssicherungen bei einer eingriffsintensiven Maßnahme wie § 11 Abs. 1a Satz 1 G 10 ist aber eine bestimmte und normenklare Regelung zu fordern.

Auch in Bezug auf die Erstreckung auf weitere Kennungen führt der weite Telekommunikationsbegriff dazu, dass sich die Grundrechtsverletzung durch den weiten Anwendungsbereich noch intensiviert. So können nach der Anordnung bezogen auf eine Rufnummer durch die Erstreckung auf weitere Kennungen auch Cloud-Bewegungen und das Surfverhalten insgesamt überwacht werden (hierzu **D.I.3.a)(2)(d)**).

(2) Unzureichende Benachrichtigungspflicht § 12 Abs. 1 G 10

§ 12 Abs. 1 Satz 1 G 10 enthält eine grundsätzliche Benachrichtigungspflicht, die auch bei Maßnahmen nach § 11 Abs. 1a Satz 1 G 10 eingreift. Allerdings statuiert § 12 Abs. 1 Satz 2 G 10 Ausnahmen von dieser Pflicht, die über das verfassungsrechtlich Erlaubte hinausgehen.

Gem. Art. 10 Abs. 2 Satz 2 GG besteht grundsätzlich die Möglichkeit, dass Beschränkungen des Fernmeldegeheimnisses den Betroffenen nicht mitgeteilt werden, wenn die Beschränkungen dem Schutz der freiheitlichen demokratischen Grundordnung oder dem Bestand oder der Sicherung des Bundes oder Landes dienen. Das angerufene Gericht hat sich mit den entsprechenden Beschränkungsmöglichkeiten insbesondere in seiner Entscheidung zur *Telekommunikationsüberwachung I* auseinandergesetzt. Demnach tritt an die Stelle der Mitteilungspflicht eine nachträgliche Benachrichtigungspflicht, sobald eine Gefährdung des Zwecks der Maßnahme und eine Gefährdung des Bestandes oder der Sicherung des Bundes oder eines Landes ausgeschlossen werden können.

Das angerufene Gericht hält eine Einschränkungsmöglichkeit der Mitteilungspflicht zudem auch über Art. 10 Abs. 2 Satz 2 GG hinaus für möglich. Derartige Beschränkungen sind dann auf Art. 10 Abs. 2 Satz 1 GG zu stützen. Das Gericht nennt in diesem Zusammenhang die behördliche Aufgabenwahrnehmung außerhalb des Schutzes der freiheitlich demokratischen Grundordnung sowie übergreifende Nachteile für das Wohl des Bundes oder eines Landes, die im Fall einer Kenntnisgewähr absehbar sind. Das Gericht konkretisiert dies dann anhand der Beispiele der Beteiligung ausländischer Nachrichtendienste, der Spionageabwehr und des Schutzes von Informationsquellen.

Vgl. BVerfGE 100, 313 <397 f.> m.w.N.

Zugleich ist davon auszugehen, dass auch bei den Beschränkungen der Mitteilungs- und Benachrichtigungspflichten die allgemeinen Grundsätze zu heimlichen Maßnahmen zur Anwendung kommen, und dementsprechend gesetzli-

che Grundlagen am Grundsatz der Bestimmtheit zu messen sind und verhältnismäßig ausgestaltet sein müssen.

Vgl. BVerfGE 154, 152 <287 Rn. 267> m.w.N.

Diesen Anforderungen wird § 12 Abs. 1 Satz 2 G 10 nicht gerecht.

Nach § 12 Abs. 1 Satz 2 G 10 unterbleibt die nachträgliche Benachrichtigung, „solange eine Gefährdung des Zweckes der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar sind."

Diese Bestimmungen sind zu unbestimmt, um die Beschränkung zu rechtfertigen. Es ist weder ersichtlich, unter welchen Umständen der Zweck der Beschränkung gefährdet sein kann, noch, was unter übergreifenden Nachteilen für das Wohl des Bundes oder eines Landes zu verstehen ist. Das angerufene Gericht verwendete zwar ebenfalls diese Terminologie, konkretisierte diese Umstände im Anschluss jedoch durch einzelne Beispiele.

BVerfGE 100, 313

Auch der Gesetzgeber hätte hier dementsprechend vorgehen und näher ausführen müssen, unter welchen Umständen der Zweck der Beschränkung gefährdet sein kann, bzw. wann ein übergreifender Nachteil für das Wohl des Bundes oder eines Landes absehbar sein können.

Zudem geht die Vorschrift in ihrer derzeitigen Ausgestaltung auch zu weit. Danach erfolgen generell keine Benachrichtigungen, wenn eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann. Es kann aber zumindest fast nie vollkommen ausgeschlossen werden, dass eine Benachrichtigung den Zweck der Beschränkung nicht gefährdet, da durch die Benachrichtigung Informationen über den Anlass einer Maßnahme zumindest geschlussfolgert werden können. Auch können sich regelmäßig Hinweise auf andere Informationsquellen ergeben, die für die Maßnahme eine Rolle gespielt haben. Hinzu kommt, dass die Einschätzung, ob eine derartige Zweckgefährdung ausgeschlossen ist, durch die durchführende Behörde autark getroffen

wird. Erfahrungsgemäß werden gerade bei Nachrichtendiensten Gefahren durch Benachrichtigungen über Maßnahmen als hoch angesehen.

Durch diese weitgehende Einschränkung kann eine Benachrichtigung praktisch für einen Großteil der Fälle – wenn nicht sogar für alle Fälle – ausgeschlossen werden. Damit wird Betroffenen faktisch das Recht genommen, sich – wenn auch nur im Nachhinein – gegen eine Maßnahme zur Wehr zu setzen. Dies ist besonders problematisch bei dem intensiven Eingriff der Quellen-Telekommunikationsüberwachung.

Auch bei Einhaltung der geforderten Voraussetzungen bestehen weiterhin – wie auch vom angerufenen Gericht anerkannt – Möglichkeiten der Einschränkungen der Benachrichtigungspflicht. Diese sind aber auf ein Maß zu beschränken, das nicht zu einem generellen Ausschluss von Benachrichtigungen führen und hinreichend kontrolliert werden kann.

Die Defizite dieser Vorschrift werden auch nicht durch andere Regelungen aufgewogen.

Zunächst garantieren die weiteren Regelungen des § 12 Abs. 1 G 10 keinen hinreichenden Grundrechtschutz. Gemäß § 12 Abs. 1 Satz 3 G 10 bedürfen die Zurückstellung einer Benachrichtigung über zwölf Monate hinaus sowie eine endgültige Unterlassung der Mitteilung der Befassung der G 10-Kommission. Nach § 12 Abs. 1 Satz 4 G 10 bestimmt die Kommission auch die Dauer der weiteren Zurückstellung. Diese unabhängige Kontrolle ist jedoch insoweit unzureichend, als dass die Kommission anhand der in § 12 Abs. 1 Satz 2 G 10 enthaltenen, unzureichenden Kriterien entscheidet.

Zudem ist nicht ersichtlich, weshalb diese erst nach zwölf Monaten zu erfolgen hat. Sollte die Mitteilung zu Unrecht unterlassen worden sein, kann sich durch die Verzögerung unter anderem eine Einbuße im Rechtsschutz des Betroffenen ergeben. Dieser kann gem. § 13 G 10 erst nach der Benachrichtigung Rechtsschutz ergreifen. Dabei ist aber zu berücksichtigen, dass bei einem zusätzlichen Ablauf von zwölf Monaten schon aus Gedächtnisgründen eine effektive gerichtliche Überprüfung der Maßnahme unwahrscheinlicher wird.

Auch darüber hinaus besteht keine Möglichkeit für Betroffene an Informationen zu kommen.

Die Nachrichtendienste sind vom Informationsfreiheitsgesetz (IFG) des Bundes und vergleichbarer Landesgesetze ausgeschlossen (§ 3 Nr. 8 IFG). Zwar sehen die gesetzlichen Grundlagen der Nachrichtendienste einzelne Auskunftsansprüche vor. Auch diese enthalten aber weitgehende Einschränkungen. So knüpft beispielsweise § 15 Abs. 2 Satz 1 Nr. 1 BVerfSchG als Versagungsgrund an die Gefährdung der Aufgabenerfüllung an. Zudem besteht das besondere Problem, dass das Artikel 10-Gesetz eine Vielzahl von Behörden ermächtigt und Betroffene daher nicht wissen, an welche Behörde sie sich beim Verdacht, dass eine Maßnahme gegen sie durchgeführt wurde, überhaupt wenden sollen.

Auch der Bericht an das Parlamentarische Kontrollgremium (PKrGr) gemäß § 14 Abs. 1 G 10 bietet keine hinreichende Kontrolle. Dieser stellt die Arbeit der Nachrichtendienste nur im groben Überblick dar. Das angerufene Gericht hat festgestellt, dass dem Kontrollgremium die politische Kontrolle im Anwendungsbereich des Artikel 10-Gesetzes lediglich im Sinne einer „allgemeinen Kontrolle über die Durchführung des G 10“ obliegt. Dabei gehe es nicht um Einzelfälle, sondern um die Gesamtübersicht der Beschränkungsmaßnahmen und Grundsatzfragen.

Vgl. BVerfGE 143, 1 <17 f. Rn. 53>.

Zwar ist nunmehr gesetzlich gefordert, dass der Bericht des PKrGr gesondert auf Anordnungen nach § 11 Abs. 1a G 10 einzugehen hat, § 14 Abs. 1 Satz 2 G 10. Auch dabei bleibt es jedoch bei einer Befassung im Überblick.

Es ist dem Parlamentarischen Kontrollgremium damit nicht möglich, einzelne Anordnungen oder unterbliebene Benachrichtigungen näher zu überprüfen. Betroffene haben hierdurch erst recht keine Möglichkeit, eine weitere Überprüfung herbeizuführen.

(3) Verfassungsrechtliche Mängel der Eilanordnung § 15a G 10

Auch durch die Regelungen zu Anordnungen bei Gefahr im Verzug werden mehr Verfahrenssicherungen ausgeschaltet, als dies verfassungsrechtlich zulässig ist.

Diesbezüglich ist ebenfalls fraglich, inwieweit in Eilfällen überhaupt auf nachrichtendienstliche Vorfeldaufklärung zurückgegriffen werden oder ob nicht Gefahrenabwehrbehörden der Vorzug gegeben werden sollte.

Wird ein derartiges Bedürfnis jedoch akzeptiert, sind Beschränkungen für Anordnungen bei Gefahr im Verzug dennoch auf ein notwendiges Maß zu begrenzen.

Dies ist bei § 15a G 10 in mehreren Hinsichten nicht der Fall.

Die Vorschrift sieht keine Dokumentationspflichten bezüglich des Eilanlasses vor. Nach § 15a Abs. 1 ist in der Anordnung zu bestimmen, dass die Zustimmung der G 10-Kommission nicht abzuwarten ist. Es ist allerdings nicht geregelt, dass der Grund für diese Bestimmung auszuführen wäre. Das beschränkt die Kontroll- und eröffnet Missbrauchsmöglichkeiten.

Zudem schränkt § 15a G 10 nicht ein, welcher Personenkreis eine derartige Entscheidung treffen darf. Um Missbrauch zu vermeiden, ist eine Person mit Befähigung zum Richteramt zu fordern. Eine derartige Beschränkung sieht das Artikel 10-Gesetz an anderer Stelle vor (wenn auch regelmäßig nur als Aufsichtsperson, so auch in § 15a Abs. 3 Satz 2 G 10).

Schließlich sieht die Norm zwar Löschpflichten vor, enthält aber kein Verwertungsverbot für den Fall, dass eine Anordnung nicht bestätigt wird.

(4) Kontrollregime ungenügend

Das angerufene Gericht fordert in ständiger Rechtsprechung für eingriffsintensive Überwachungsbefugnisse, dass eine unabhängige Vorabkontrolle bestehen muss. Eine solche besteht zwar im Grundsatz mit der G-10 Kommission

nach § 15 G 10. Jedoch erfüllt diese im nicht alle Voraussetzungen, die an eine derartige Kontrollinstanz zu stellen sind.

(a) Maßstäbe

(i) Notwendigkeit einer Vorabkontrolle

Nach der Rechtsprechung des angerufenen Gerichts steht gerade bei nachrichtendienstlichen Maßnahmen der unabhängigen Kontrolle eine besondere Bedeutung zu, da derartige Befugnisse bereits im Vorfeld von Gefahren im Sinne des Polizeirechts möglich sind.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 213.

Ob eine solche Kontrolle für eine konkrete Befugnis zu fordern ist, richtet sich nach der Eingriffsintensität. Abzustellen ist dabei neben der Heimlichkeit maßgeblich darauf, ob es sich um Maßnahmen handelt, bei denen damit zu rechnen ist, dass sie auch höchstprivate Informationen erfassen.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 217. Dazu auch EGMR, Urteil vom 6. September 1978, Nr. 5029/ 71, § 56; EGMR, Urteil vom 4. Dezember 2015, Nr. 47143/06, §§ 258, 275; EGMR, Urteil vom 12. Januar 2016, Nr. 37138/14, § 77.

Diese Kriterien treffen auf die Quellen-Telekommunikationsüberwachung nach § 11 Abs. 1a Satz 1 G 10 zu, sodass eine unabhängige Vorabkontrolle erforderlich ist. Denn zunächst wird auch die Quellen-Telekommunikationsüberwachung heimlich durchgeführt. Zudem ermöglicht die Überwachung der laufenden Telekommunikation auch die Erfassung höchstprivater Informationen. Zudem bestehen zwar Höchstgrenzen für einzelne Anordnungen, aber keine Begrenzungen hinsichtlich einer Maximaldauer durch Aneinanderreihung mehrerer Anordnungen, sodass es auch zu langfristigen Überwachungen kommen kann.

> Vgl. auch BVerfGE 100, 313 <361, 401>.

(ii) Anforderungen an Vorabkontrolle

Nach der Rechtsprechung des angerufenen Gerichts hat der Gesetzgeber die unabhängige Kontrolle in spezifischer und normenklarer Form zu regeln. Die Regelung muss das Erfordernis einer hinreichend substantiierten Begründung des von der Behörde zu stellenden Antrags auf Anordnung enthalten, die es überhaupt erst praktisch erlaubt, eine unabhängige Kontrolle effektiv auszuüben. Zudem muss die antragstellende Behörde verpflichtet werden, über alle beurteilungsrelevanten Aspekte zu informieren. In Anknüpfung hieran ist die Aufgabe und Pflicht der unabhängigen Stelle zu regeln, sich eigenverantwortlich ein Urteil darüber zu bilden, ob die beantragte heimliche Überwachungsmaßnahme den gesetzlichen Voraussetzungen entspricht. Hierfür sind die notwendigen sachlichen und personellen Voraussetzungen zu schaffen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 215.

Konkretere Ausführungen zu Anforderungen an gerichtsähnliche Kontrollen machte das angerufene Gericht in seiner Entscheidung zur *Auslands-Auslands-Aufklärung*. Danach ist die gerichtsähnliche Kontrolle – neben einer administrativen Kontrolle – Teil der objektiven Rechtskontrolle, die für eine strategische Auslandsaufklärung notwendig ist.

Vgl. BVerfGE 154, 152 <290 ff. Rn. 272 ff.>.

Konkret führte das Gericht diesbezüglich aus, dass für die gerichtsähnliche Kontrolle Spruchkörper vorzusehen sind, die mit Personen in gleichsam richterlicher Unabhängigkeit besetzt sind und in formalisierten Verfahren schriftlich und abschließend mit Wirkung für Bundesregierung und Nachrichtendienst entscheiden. Diese Kontrolle hat die Schutzaufgabe zu erfüllen, die sonst dem Richtervorbehalt sowie auch nachträglichen Rechtsschutzmöglichkeiten, insbesondere Feststellungsklagen, zukommt. Entsprechend muss mit ihr eine auf den Einzelfall bezogene Prüfung ermöglicht werden, die materiell und verfahrensmäßig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll ist.

BVerfGE 154, 152 <291 Rn. 275>.

Die konkrete Ausgestaltung muss dabei an der wirksamen und unabhängigen Aufgabenerfüllung orientiert sein.

Vgl. BVerfGE 154, 152 <294 Rn. 283>.

Dies bedeutet, dass für die berufenen Mitglieder sicherzustellen ist, dass diese einer der richterlichen Unabhängigkeit gleichkommenden Unabhängigkeit innehaben. Sie müssen weisungsfrei und auf hinreichend lange und bestimmte Zeit fest berufen sein. Für die Zusammensetzung der Spruchkörper ist zu gewährleisten, dass der richterlichen Perspektive ein maßgebliches Gewicht zukommt, indem eine maßgebliche Zahl der Mitglieder über langjährige richterliche Erfahrung verfügen muss. Das schließt nicht aus, Erfahrungen aus anderen juristischen Berufen zu berücksichtigen. In Betracht zu ziehen ist auch, dass zusätzlich möglicherweise anderweitiger insbesondere technischer Sachverstand förderlich sein kann. Es liegt in den Händen des Gesetzgebers zu entscheiden, ob er hierfür Mitglieder des gerichtsähnlichen Entscheidungsgremiums – unter Umständen abhängig von der Art der Entscheidung – ergänzend auch Nichtjurist*innen vorsieht, oder ob er dem Gremium anderweitige Möglichkeiten an die Hand gibt, technischen Sachverstand heranzuziehen.

Vgl. BVerfGE 154, 152 <295 Rn. 286>.

Es ist eine fachlich kompetente, professionalisierte Kontrolle durch grundsätzlich hauptamtlich tätige Personen sicherzustellen. Es reicht nicht, die Durchführung der Kontrolle im Wesentlichen auf eine ehrenamtliche Amtsausübung zu stützen. Zugleich ist auf eine ausgewogene Zusammensetzung zu achten. Personell wie strukturell ist zur Sicherstellung der gebotenen Unabhängigkeit auf die Wahrung einer hinreichenden Distanz zum BND zu achten.

BVerfGE 154, 152 <295 Rn. 287>.

Auch wenn das angerufene Gericht diese Grundsätze explizit nur für den BND im Bereich der strategischen Auslandsaufklärung aufgestellt hat, ergibt sich kein Grund, weshalb diese Grundsätze nicht auch auf die unabhängige Kontrolle nachrichtendienstlichen Handelns im Inland zu übertragen sein.

Im Kern führte das angerufene Gericht im Wesentlichen aus, was unter einer gerichtsähnlichen Kontrolle zu verstehen ist. So dienen die ausgearbeiteten Elemente auch gerade der Wirksamkeit und Unabhängigkeit der Kontrolle. Diese ist aber universell zu fordern und nicht ausschließlich mit Bezug auf den BND.

Auch die konkreten Defizite, die durch die objektiv-rechtliche Kontrolle ausgeglichen werden sollen, gelten ebenso für die anderen Nachrichtendienste bei deren inländischen Tätigkeit nach dem Artikel 10-Gesetz.

So dient die objektiv-rechtliche Kontrolle zunächst dem Ausgleich der Rechtsschutzdefizite im Bereich der Auslands-Auslands-Fernmeldeaufklärung. In diesem Bereich gelten nur sehr begrenzte Auskunfts- und Benachrichtigungspflichten, sodass Betroffene Maßnahmen regelmäßig keiner Überprüfung zuführen können.

BVerfGE 154, 152 <290 Rn. 273>.

Auch im Bereich der innerstaatlichen Maßnahmen besteht ein vergleichbares Defizit. So besteht keine vorherige Mitteilungspflicht (§ 12 G 10). Nachträgliche Benachrichtigungen sind ebenfalls regelmäßig ausgeschlossen (hierzu **(2)**).

Eine objektiv-rechtliche Kontrolle ist zudem notwendig, da im Bereich der Auslands-Auslands-Fernmeldeaufklärung im Wesentlichen nur eine finale Anleitung der Überwachungsbefugnisse stattfindet und daher die verfahrensmäßige Strukturierung der Handhabung dieser Befugnisse abzusichern ist.

BVerfGE 154, 152 <290 Rn. 273>.

Zwar erfolgen die Maßnahmen des § 11 Abs. 1a G 10 grundsätzlich zielgerichteter als die strategische Auslandsaufklärung. Die Entscheidung des angerufenen Gerichts bezieht sich aber auch auf zielgerichtete Maßnahmen gegen (dem Dienst bekannte und gezielt angesteuerte) Einzelpersonen. Auch Maßnahmen

gegen sie müssen ex ante einer gerichtsähnlichen Kontrolle unterzogen werden.

BVerfGE 154, 152 <258 Rn. 188>.

Dies muss dann erst recht für die eingriffsintensiveren Fälle des § 11 Abs. 1a G 10 gelten. Sie ermöglichen eine umfassendere Überwachung der Zielperson, da im Inland bessere Überwachungsmöglichkeiten bestehen. So ist es dem BND im Ausland in der Regel nicht möglich, den vollständigen Telekommunikationsverkehr abzugreifen. Zudem ist die Quellen-Telekommunikationsüberwachung durch den Zugriff auf informationstechnische Systeme gegenüber anderen Überwachungsmaßnahmen ein wesentlich einschneidenderes Mittel. Hinzu kommt, dass bei den Maßnahmen im Inland Folgemaßnahmen drohen, die im Ausland regelmäßig nicht möglich sind.

Dementsprechend besteht sogar ein gegenüber der Auslands-Auslands-Fernmeldeaufklärung stärkeres Bedürfnis an verfahrensrechtlicher Absicherung; mindestens die oben zitierten Vorgaben des angerufenen Gerichts an die gerichtsähnliche Kontrolle sind jedoch einzuhalten.

Diese Voraussetzungen werden auch nicht durch die Ausführungen des angerufenen Gerichts im seiner Entscheidung zum *Bayerischen Verfassungsschutzgesetz* relativiert. Auch in diesem Verfahren hat das Gericht bei eingriffsintensiven Maßnahmen eine unabhängige Vorabkontrolle gefordert, hat dort aber nicht dieselben hohen Anforderungen der Auslands-Auslands-Fernmeldeaufklärung wiederholt. Dazu hatte das angerufene Gericht aber auch keinen Anlass. Die Befugnis zur Quellen-Telekommunikationsüberwachung war nicht Gegenstand der Entscheidung. Nach dem Bayerischen Verfassungsschutzgesetz bedurfte es für die vergleichbar intensiven Maßnahmen der Wohnraumüberwachung und der Online-Durchsuchung sogar einer richterlichen Anordnung, § 11 Abs. 1 Satz 1 BayVSG. Insoweit das Gericht dabei konkreten Bezug auf die G-10 Kommission genommen hatte, ging es nur darum, dass grundsätzlich auch ein geheimes Verfahren möglich ist.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 224.

(b) G 10-Kommission entspricht Anforderungen nicht

Die G 10-Kommission genügt den entwickelten Maßstäben nicht. Ein Vergleich der Kommission mit dem Unabhängigen Kontrollrat des BNDG-Regimes (§§ 40 ff. BND-Gesetz (BNDG)) macht die Defizite deutlich.

Beim Unabhängigen Kontrollrat ist entscheidend, dass Personen in gleichsam richterlicher Unabhängigkeit in formalisierten Verfahren schriftlich und mit bindender Wirkung für die Nachrichtendienste entscheiden. Im Gegensatz dazu sind die Anordnungen von Beschränkungen zwar durch die G 10-Kommission zu bestätigen (§ 15 Abs. 6 Satz 1 G 10), allerdings mangelt es bereits an der erforderlichen gerichtsähnlichen Ausgestaltung der Kommission. Die Mitglieder der Kommission sind zwar in ihrer Amtsführung unabhängig und Weisungen nicht unterworfen (§ 15 Abs. 1 Satz 3 G 10). Jedoch sichert § 15 G 10 nicht den notwendigen Grad an Professionalisierung, der von Mitgliedern eines derartigen Gremiums zu fordern ist.

Vgl. hierzu *Bantlin*, Die G10-Kommission – Zur Kontrolle der Nachrichtendienste, 1. Aufl. 2021, S. 154 f.

Der Unabhängige Kontrollrat ist ausschließlich mit Personen besetzt, die vor ihrer Ernennung als Richter*innen am Bundesgerichtshof oder am Bundesverwaltungsgericht tätig waren und in dieser Tätigkeit über langjährige Erfahrung verfügen (§ 43 Abs. 1 BNDG). Damit wird die vom angerufenen Gericht geforderte richterliche Perspektive sichergestellt. Für die G 10-Kommission lässt § 15 Abs. 1 Satz 2 G 10 die Befähigung zum Richteramt ausreichen.

Während der Unabhängige Kontrollrat damit ausschließlich mit Jurist*innen besetzt ist, ist im Rahmen der G 10-Kommission lediglich bei drei von fünf Mitgliedern der Kommission und drei von fünf Mitgliedern der Stellvertreter*innen notwendig, dass diese die Befähigung zum Richteramt besitzen. Das ist in zwei Hinsichten problematisch.

Erstens regelt § 15 G 10 selbst nichts Näheres zu den Vertretungsregelungen. Dementsprechend ist nicht hinreichend bestimmt ausgeschlossen, dass durch Vertretungsfälle der überwiegende Teil der Kommission von Jurist*innen besetzt ist. Damit ist nicht – wie vom angerufenen Gericht gefordert – sichergestellt, dass der richterlichen Perspektive ein maßgebliches Gewicht zukommt.

Zweitens erlaubt das angerufene Gericht zwar auch die Besetzung mit Jurist*innen. Aus den Ausführungen des Gerichts wird aber deutlich, dass dies einem Zweck zu dienen hat. Das Gericht selbst stellt auf vorhandenes technisches Wissen ab. Derartige Anforderungen stellt § 15 G 10 nicht. Vielmehr stellt dieser überhaupt keine Bedingungen an die nichtjuristischen Mitglieder auf. Damit wird eine hinreichende Professionalisierung des Gremiums nicht sichergestellt.

Zudem nehmen die Mitglieder der G 10-Kommission ein öffentliches Ehrenamt wahr, § 15 Abs. 1 Satz 4 G 10. Das angerufene Gericht lässt eine derartige ehrenamtliche Ausübung aber gerade nicht ausreichen und fordert vielmehr eine grundsätzlich hauptamtliche Ausübung.

(c) Änderungen nicht weitgehend genug

Zwar wurde im Rahmen des Gesetzes zur Anpassung des Verfassungsschutzrechts auch § 15 G 10 überarbeitet. Diese Überarbeitungen waren jedoch ungenügend. Neben einer Erweiterung der Rechte in § 15 Abs. 5 Satz 4 G 10 und der prozessualen Stärkung in § 15 Abs. 6 G 10 betrifft dies insbesondere die Zusammensetzung der Kommission. So musste zuvor lediglich der*die Vorsitzende die Befähigung zum Richteramt besitzen. Damit liegen durch die Änderungen weitergehende Professionalisierungsanforderungen vor. Diese sind jedoch dennoch unzureichend, unter anderem, da die Befähigung zum Richteramt nicht ausreichend ist, um die Anforderungen zu erfüllen.

d) Mängel nicht durch Neuerungen des G 10-Gesetzes ausgeglichen

Im Rahmen der angegriffenen Gesetzesänderungen kam es auch zu einer Erweiterung der Rechte der G 10-Kommission, insbesondere durch die Neufassung des § 15 G 10. Jedoch reichen diese nicht aus, um die Mängel der geschaffenen Eingriffsgrundlage zu kompensieren. Zunächst bleibt das Kontrollregime des Artikel 10-Gesetzes insgesamt hinter den Anforderungen an eine effektive Rechtskontrolle zurück (hierzu **c)(4)**). Darüber hinaus könnten auch hervorragende Kontrollbefugnisse nicht die allgemeinen Mängel im Bereich der Voraussetzungen zum Einsatz der Quellen-Telekommunikationsüberwachung kompensieren. Sind diese zu niedrig angesetzt, kann eine Kontrollinstanz daran nichts mehr ändern.

II. Beschränkte Online-Durchsuchung (§ 11 Abs. 1a Satz 2 G 10)

§ 11 Abs. 1a Satz 2 G 10 ermächtigt die Behörden, neben der laufenden auch auf die auf den informationstechnischen Systemen gespeicherte Kommunikation zuzugreifen. Diese Befugnis zur beschränkten Online-Durchsuchung verletzt die Beschwerdeführer*innen in ihrem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Entgegen der Auffassung des Gesetzgebers ist § 11a Abs. 1a Satz 2 G 10 nicht an den Maßgaben des Fernmeldegeheimnisses zu messen, sondern an jenen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (hierzu **1**). Hieraus ergeben sich besondere Anforderungen, die der Gesetzgeber verkannt hat (hierzu **2.a)**). Darüber hinaus leidet § 11 Abs. 1a Satz 2 G 10 an den gleichen verfassungsrechtlichen Mängeln wie bereits § 11 Abs. 1a Satz 1 G 10 (hierzu **2.b)**).

1. Beschränkte Online-Durchsuchung greift in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein

Nach der Rechtsprechung des angerufenen Gerichts handelt es sich bei einer Online-Durchsuchung um einen Eingriff in das allgemeine Persönlichkeitsrecht als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Zwar besteht eine Bereichsausnahme hinsichtlich Eingriffen in die Telekommunikation, sodass insofern Art. 10 Abs. 1 GG zum Tragen kommt. Diese Ausnahme greift jedoch nur so weit, wie der Zugriff auf laufende Kommunikation begrenzt ist. Ein darüber hinausgehender Zugriff ist an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu messen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 308.

Auch § 11 Abs. 1a Satz 2 G 10 ist mithin als Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu qualifizieren.

Die Vorschrift ermöglicht den Zugriff auf gespeicherte Daten mit zwei Einschränkungen. Erstens darf nur auf Informationen zugegriffen werden, wenn diese auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

Zweitens darf nur auf Informationen zugegriffen werden, die nach der Anordnung gespeichert wurden.

Beide Einschränkungen führen nicht dazu, dass die Befugnis nicht als Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu qualifizieren ist.

Die Vorschrift knüpft mit der ersten Einschränkung an die Möglichkeit der Quellen-Telekommunikationsüberwachung in Satz 1 an. Daraus ergibt sich die Beschränkung, dass auch Satz 2 nur einen Zugriff auf Telekommunikationsdaten ermöglicht wird. Dieser ist aber nicht auf die laufende Telekommunikation beschränkt, sondern geht darüber hinaus. Während bei Satz 1 gerade die Überwachung und Aufzeichnung ermöglicht wird, umfasst Satz 2 Fälle, in denen dies nicht möglich war und ermöglicht als Ausgleich den Zugriff auf die gespeicherte Kommunikation. Damit handelt es sich aber gerade um einen Zugriff auf die ruhende Kommunikation und damit nach der Kategorisierung des angerufenen Gerichts um einen Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

> Vgl. *Roggan*, DVBl 2021, 1471 (1474); *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste, Verfassungsblog vom 6. Juli 2021, abrufbar unter https://verfassungsblog.de/staatstrojaner-nachrichtendienste/; zur vergleichbaren Vorschrift § 100a StPO *Brodowski*, in: BeckOK IT-Recht, 1. Aufl. 2020, StPO, § 100a Rn. 10; *ders./Sieber*, in: Hoeren/Sieber/Holznagel MMR-HdB, 54. EL Oktober 2020, Teil 19.3

Strafprozessrecht, Rn. 151; *Martini/Fröhlingsdorf*, NVwZ 2020, 1803; *Großmann*, JA 2019, 241 (243); *Freiling/Safferling/Rückert*, JR 2018, 9 (21); *Singelnstein/Derin*, NJW 2017, 2646 (2648).

Dass ein Zugriff auf ruhende Kommunikation vorliegt, wird auch durch die Gesetzesbegründung unterstrichen. Danach dient die Befugnis zur Schließung der Aufklärungslücke bei Messenger-Diensten für Daten aus dem Speicher des Zielsystems, die technisch unverschlüsselt ausgelesen werden sollen.

Vgl. BT-Drucks. 19/24785, 22.

Eine weitergehende Auseinandersetzung, weshalb es sich bei dieser Art der beschränkten Online-Durchsuchung um einen Zugriff auf die laufende Kommunikation handeln sollte, erfolgt jedoch nicht, obwohl sämtliche juristischen Stellungnahmen im Gesetzgebungsverfahren auf die Rechtsprechung des angerufenen Gerichts hingewiesen haben.

Vgl. die Stellungnahmen von *Bäcker*, zu dem Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts (BT-Drs. 19/24785), Ausschuss-Drs. 19(4)844 A; *Graulich*, für die Öffentliche Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestags am Montag, 17. Mai 2021, 12.00 Uhr zum Gesetzentwurf der Bundesregierung für ein Gesetzes zur Anpassung des Verfassungsschutzrechts (BT-Drs. 19/24785), Ausschuss-Drs. 19(4)844 C; *Rusteberg*, zur Vorbereitung der öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung (BT-Drs. 19/24785, 19/24900), Ausschuss-Drs. 19(4)844 D; *Poscher*, zu dem Entwurf der Bundesregierung eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Ausschuss-Drs. 19(4)844 E. Darauf hinweisend, wenn auch zurückhaltender, *Dietrich*, zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts“ (BT-Drucksache 19/24785, 19/24900), Ausschuss-Drs. 19(4)844 F.

> Auch die zweite – zeitliche – Einschränkung ändert nichts daran, dass ein Zugriff auf ruhende Kommunikation vorliegt. Dass durch diese Einschränkung faktisch nur auf die gleiche Kommunikation zugegriffen werden kann, die bereits als laufende Kommunikation überwacht werden könnte und sich dementsprechend kein intensiverer Eingriff als bei der Quellen-Telekommunikationsüberwachung vorliegt, überzeugt nicht.

So kann ausweislich der Gesetzesbegründung auf diese Kommunikation eben nicht durch die Quellen-Telekommunikationsüberwachung zugegriffen werden.

Auch darüber hinaus stellen sich aber die Überwachung nach Satz 1 und die Durchsuchung nach Satz 2 quantitativ und qualitativ äußerst unterschiedlich dar. Denn die Behörden sind bei einer beschränkten Online-Durchsuchung nicht gezwungen, mit hohem Aufwand pausenlos mitzuhören oder -lesen, um die Kommunikation vollständig zu überwachen oder zuvor selbst aufgezeichnete Kommunikation im Nachhinein auszuwerten. Sie benötigen einen Bruchteil des Aufwands, um zu einem von ihnen bestimmten Zeitpunkt in wenigen Sekunden faktisch die gesamte in einem längeren Zeitraum gelebte Kommunikation einzusehen. Diese enorme Vereinfachung erhöht die Bereitschaft zur Nutzung der Befugnis und damit die Wahrscheinlichkeit solcher Eingriffe faktisch erheblich.

Des Weiteren nähert sich die Kommunikation mittels Text- und Sprachnachrichten in einem Messenger in der praktischen Handhabung sehr stark der Flüchtigkeit der gesprochenen Sprache an. Die Nutzer*innen wenden hier typischerweise gerade nicht die erhöhte Sorgfalt auf, die herkömmlicherweise auf schriftliche Äußerungen gerade deshalb gerichtet wird, weil jene verkörpert und damit beständig sind. Die Überwachung der aufgezeichneten Chat-Kommunikation weist diesen Äußerungen nachträglich ein Gewicht zu, das die Betroffenen selbst ihnen im Moment der Kommunikation typischerweise gerade nicht zugemessen haben.

2. Maßstab der „klassischen“ Online-Durchsuchung ist auf die beschränkte Online-Durchsuchung zu übertragen.

Nach der Rechtsprechung des angerufenen Gerichts liegt mit einer „klassischen“, also unbeschränkten, Online-Durchsuchung auch ein intensiver Eingriff vor. Dies hat das Gericht zuletzt in seiner Entscheidung zum *Bayerischen Verfassungsschutzgesetz* bestätigt. Danach liegt bei der klassischen Online-Durchsuchung eine Konstellation vor, bei der bereits der Eingriff derart intensiv ist, dass für nachrichtendienstliche und gefahrenabwehrrechtliche Befugnisse dieselben Anforderungen gelten.

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 168.

Diese Maßstäbe sind auf die beschränkte Online-Durchsuchung zu übertragen. Auch wenn diese terminologisch auf gespeicherte Telekommunikation beschränkt ist, steht diese der klassischen Online-Durchsuchung im Eingriffsgewicht kaum nach.

Zunächst ist unklar, bei welchen auf einem System gespeicherten Daten es sich überhaupt um Telekommunikation handelt. Das kann sich erst durch eine Sichtung und Überprüfung der Dateien ergeben. Mithin startet auch die beschränkte Online-Durchsuchung als klassische Online-Durchsuchung mit einem Vollzugriff auf das System. Erst auf einer zweiten Stufe werden dann Informationen ausgesiebt. Damit besteht die Möglichkeit, dass es zu Fehlern oder Missbrauch bei der Aussonderung kommt.

So betont das angerufene Gericht in seiner Rechtsprechung auch, dass bei der klassischen Online-Durchsuchung durch die Infiltration des Systems bereits die entscheidende Hürde genommen wurde, um das System insgesamt auszuspähen und damit auch weitere persönlichkeitsrelevante Informationen zu erheben.

> Vgl. BVerfGE 120, 274 <308 f.>; siehe hierzu auch *Roggan*, DVBl 2021, 1471 (1474).

Eine Infiltration nur der Telekommunikationsdaten ist nicht möglich.

Zudem stellt das angerufene Gericht im Rahmen der klassischen Online-Durchsuchung heraus, dass diese von besonderer Intensität ist, da sie das Risiko einer weitgehenden Ausspähung der Persönlichkeit birgt.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 168.

Dieses Risiko liegt aber auch bei der Beschränkung auf Telekommunikationsdaten vor. So lassen sich Anhaltspunkte zur Persönlichkeit einer Person regelmäßig insbesondere aus deren Kommunikation mit anderen Personen ablesen. Hier werden private Gedanken, Wünsche und Pläne geäußert. Zwar besteht die grundsätzliche Möglichkeit, dass derartige Informationen auch in Dateien gespeichert sind, die nicht der Kommunikation dienen. Diese theoretische Möglichkeit darf aber nicht dazu führen, dass die höchst sensiblen Telekommunikationsdaten einem geringeren Schutzniveau unterliegen.

Zudem ergibt sich nach dem angerufenen Gericht die besondere Intensität des Grundrechtseingriffs nicht ausschließlich aus der großen Menge an Informationen, auf die im Rahmen der klassischen Online-Durchsuchung zugegriffen werden kann. Vielmehr sind hier auch die Heimlichkeit der Maßnahme, der Umstand, dass Schutzvorkehrungen umgangen werden, sowie die Streubreite zu berücksichtigen.

Vgl. BVerfGE 120, 274 <322 ff.>.

Diese intensitätssteigernden Faktoren gelten auch bei § 11 Abs. 1a Satz 2 G 10 unverändert fort.

Schließlich führt auch der weite Telekommunikationsbegriff dazu, dass die beschränkte Online-Durchsuchung faktisch nicht begrenzt ist. So stellen der Up- und Download von Dateien Telekommunikation dar. Damit erweitert dieser Begriff den Umfang an Daten, auf die zugegriffen werden kann. So ist eben nicht nur der Zugriff auf Nachrichten aus Messenger-Diensten möglich, sondern vielmehr der Zugriff auf sämtliche Dateitypen (siehe hierzu **I.3.a)(2)(d)**).

Auch die Einschränkung auf Inhalte, die nach der Anordnung gespeichert wurden, bewirkt keine Einschränkung, die einer Übertragung der Grundsätze der klassischen Online-Durchsuchung entgegenstehen würde.

So findet heutzutage ein erheblicher Anteil an Kommunikation über informationstechnische Systeme statt. Auch wenn also im Zeitpunkt der Anordnung selbst noch auf keine Inhalte zugegriffen werden kann, wächst die Zahl der Daten, auf die zugegriffenen werden kann, sodann rapide an und ermöglicht schnell eine Erfassung der Persönlichkeit der Nutzer*innen. Dass vergangene Inhalte ausgeschlossen sind, ist insofern nicht von größerer Relevanz, da gerade die aktuellen Inhalte zur Erfassung der Persönlichkeit von besonderer Relevanz sind.

Schließlich führt der weite Telekommunikationsbegriff dazu, dass sich die zeitliche Einschränkung faktisch nicht auswirkt. Aufgrund der Regelmäßigkeit, mit der es zu Datenbewegungen im Rahmen von Up- und Downloads oder im Rahmen vom Cloud-Computing kommt, kann in kürzester Zeit auf eine Vielzahl an Dateien zugegriffen werden, auch wenn diese vor geraumer Zeit erstellt wurden. Dabei werden insbesondere relevante Dateien eher neu hoch- oder heruntergeladen werden. Im Fall der Nutzung eines neuen Systems mit Cloud-Speicher ist es sogar möglich, dass auf sämtliche Dateien im System zugegriffen werden kann, da diese vollkommen synchronisiert werden.

a) Verkennung der besonderen Anforderungen aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Nach der Rechtsprechung des angerufenen Gerichts darf eine klassische Online-Durchsuchung durch die Nachrichtendienste nur zur Abwehr einer mindestens konkretisierten Gefahr im polizeilichen Sinne (hierzu **(1)**) für ein besonders gewichtiges Rechtsgut (hierzu **(2)**) zugelassen werden, wobei dem Nachrichtendienst lediglich eine subsidiäre Befugnis (hierzu **(3)**) eingeräumt werden darf. Zudem bedarf es für einen effektiven Kernbereichsschutz der Vorlage sämtlicher erhobener Daten (hierzu **(4)**). Außerdem darf die Maßnahme sich nur eingeschränkt gegen nicht verantwortliche Personen richten

(hierzu **(5)**). Schließlich kann der Rechtsschutz in Bezug auf Eingriffe in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht im gleichen Maße eingeschränkt werden, wie dies bei Eingriffen in das Fernmeldegeheimnis der Fall ist (hierzu **(6)**).

Diesen Vorgaben wird § 11 Abs. 1a Satz 2 G 10 nicht gerecht.

(1) Eingriffsschwelle

Das angerufene Gericht sieht in der klassischen Online-Durchsuchung eine Maßnahme, die auch bei Durchführung durch Nachrichtendienste von einer erheblichen Intensität gekennzeichnet ist. Daraus ergibt sich, dass sich eine Modifizierung der Eingriffsschwelle verbietet. Demnach ist zu fordern, dass die Maßnahme nur zur Abwehr einer mindestens konkretisierten Gefahr im polizeilichen Sinne erfolgen darf.

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 176 ff., 310.

Dies bedeutet, dass bestimmte Tatsachen bereits den Schluss zum einen auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 176 m.w.N.

§ 3 Abs. 1 G 10 verfehlt diese Anforderungen in jeglicher Hinsicht. So bedarf es bereits keiner bestimmter Tatsachen, sondern lediglich tatsächlicher Anhaltspunkte. Darüber hinaus wird gerade keine konkretisierte Gefahr gefordert, sondern lediglich ein Verdacht, sodass noch in keiner Weise ein bestimmtes Geschehen absehbar sein muss. Schließlich reicht als Anlass für eine Maßnahme sogar aus, dass dieser Verdacht lediglich auf die Planung einer Straftat hindeutet.

So auch *Roggan*, DVBl 2021, 1471 (1474); *Huber*, in: Erbs/Kohlhaas, G 10, 239. EL Dezember 2021, § 3 Rn. 4ff; *ders.*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, G 10, § 3 Rn. 5.

(2) Geschützte Rechtsgüter

Hinsichtlich der zu schützenden Rechtsgüter bleibt § 11 Abs. 1a Satz 2 G 10 ebenso wie die Ermächtigung zur Quellen-Telekommunikationsüberwachung hinter den verfassungsrechtlichen Vorgaben zurück.

Die Maßnahme darf nur zum Schutz überragend wichtiger Rechtsgüter ergriffen werden. Hierzu zählen Leib, Leben und Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Vgl. BVerfGE 120, 274 <328 Rn. 247>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 158, 166.

§ 11 Abs. 1a Satz 2 G 10 i.V.m. § 3 Abs. 1 G 10 verfehlt diese Anforderungen in materieller Hinsicht, als die in Bezug genommenen Straftaten nicht lediglich überragend wichtige, sondern auch sonstige Individual- und Universalrechtsgüter schützen (hierzu **I.3.a)(2)(c)**).

So im Ergebnis auch *Roggan*, DVBl 2021, 1471 (1474).

§ 3 Abs. 1 G 10 überschreitet auch die Grenzen der Verhältnismäßigkeit im engeren Sinne, indem dieser Delikte aus dem Bereich mittlerer sowie der Bagatellkriminalität für eine Überwachungsmaßnahme von größter Intensität ausreichen lässt (hierzu **I.3.a)(2)(c)**).

(3) Keine Subsidiaritätsklausel vorhanden

Zudem bedarf es einer Subsidiaritätsklausel, nach der die Nachrichtendienste nur dann vorgehen dürfen, wenn polizeiliche Hilfe nicht rechtzeitig in An-

spruch genommen werden kann (so beispielsweise § 9 Abs. 2 Satz 1 BVerfSchG).

Das angerufene Gericht begründet dieses Erfordernis damit, dass auf diese Art und Weise möglichst wenigen Behörden Informationen offenbart werden. Für den Fall, dass die Nachrichtendienste selbst die Maßnahme durchführen und dadurch Informationen über eine Gefahr erlangen, können diese mangels exekutiver Befugnisse die Gefahr selbst aber nicht abwehren. In diesem Fall müssten die Nachrichtendienste dementsprechend die gesammelten Informationen an die Gefahrenabwehrbehörden weiterreichen. Hierdurch kommt es zu einem zweiten, eigenständigen Grundrechtseingriff, was die Grundrechtsbeeinträchtigung intensiviert. Diese intensivierte Grundrechtsbeeinträchtigung lässt sich verhindern, wenn die Gefahrenabwehrbehörden bereits selbst die Maßnahme durchführen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 168.

Eine Subsidiaritätsklausel aber fehlt im G 10 für die Quellen-Telekommunikationsüberwachung und die beschränkte Online-Durchsuchung.

(4) Kernbereichsschutz

Auch der Kernbereichsschutz ist unzureichend ausgestaltet. Nach der Rechtsprechung des angerufenen Gerichts sind sowohl Maßnahmen auf Erhebungs- als auch auf Auswertungsebene zu fordern.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 277.

Bei Eingriffen in informationstechnische Systeme ist dabei auf Erhebungsebene zu fordern, dass technische Mittel eingesetzt werden, um die Erhebung von kernbereichsrelevanten Informationen soweit möglich auszuschließen.

BVerfGE 120, 274 <338 Rn. 281>.

Auf Auswertungsebene ist zudem zu fordern, dass sämtliche Aufzeichnungen vor einer Kenntnisnahme durch die Behörde von einer unabhängigen Stelle auf ihre Kernbereichsrelevanz hin gesichtet werden.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 306, 315.

Diesen Anforderungen wird § 3a G 10 nicht gerecht.

Anders als beispielsweise Art. 10 Abs. 2 Nr. 3 BayVSG sieht § 3a G 10 keine technischen Maßnahmen vor, um die Erhebung von kernbereichsrelevanten Informationen auszuschließen. Auch § 11 Abs. 1a G 10 enthält derartige Sicherungen nicht.

Auch auf Verwertungsebene sind die Vorgaben des § 3a G 10 unzureichend. So sieht § 3a Abs. 1 Satz 4 zwar vor, dass automatische Aufzeichnungen nach Satz 3 (Aufzeichnungen bei Zweifeln bezüglich kernbereichsrelevanter Informationen) vorzulegen sind. Damit sind aber nicht sämtliche Aufzeichnungen erfasst, wie das Gericht auch in seiner Entscheidung zum *Bayerischen Verfassungsschutzgesetz* beanstandete, das auf § 3a Abs. 1 Satz 4 G 10 verwies.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 306.

(5) Nicht verantwortliche Dritte

Nach der Rechtsprechung des angerufenen Gerichts ist ein Vorgehen gegen nicht verantwortliche Personen, also gegen diejenigen, die nicht selbst für die Gefahr verantwortlich sind, nur in äußerst engen Grenzen möglich. So kann eine Online-Durchsuchung auf informationstechnische Systeme Dritter nur erstreckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert und ein auf ihre eigenen Systeme beschränkter Zugriff zur Erreichung des Ziels nicht ausreicht. Zudem bedarf es einer spezifischen individuellen Nähe der dritten Person zur Gefahr, in dem Sinne, dass der Kontakt zur Zielperson einen Bezug zum Ermittlungsziel aufzuweisen hat.

Vgl. BVerfGE 141, 220 <273 f.>.

Dem wird § 3 Abs. 2 Satz 2 G 10 nicht gerecht. Danach dürfen Maßnahmen auch gegen Dritte gerichtet werden, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass diese für die Zielperson bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben oder dass die Zielperson ihren Anschluss benutzt. Damit besteht gerade kein Erfordernis einer Nähebeziehung, insbesondere nicht in der Hinsicht, dass ein Bezug zum Ermittlungsziel bestehen muss.

> Siehe auch *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste, Verfassungsblog vom 6. Juli 2021, abrufbar unter https://verfassungsblog.de/staatstrojaner-nachrichtendienste/.

(6) Ausschluss des Rechtsschutzes

Hinsichtlich des Fernmeldegeheimnisses ermöglicht Art. 10 Abs. 2 Satz 2 GG den Ausschluss des Rechtsweges, wenn die Beschränkungen dem Schutze der freiheitlichen demokratischen Grundordnung oder dem Bestand oder der Sicherung des Bundes oder eines Landes dienen. Einfachgesetzlich wird dies in § 13 G 10 umgesetzt, der den Rechtsweg vor Mitteilung an Betroffene ausschließt.

Eine derartige verfassungsrechtliche Grundlage fehlt jedoch in Hinsicht auf das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Vielmehr ergibt sich bei diesem Recht in Verbindung mit der Rechtsweggarantie des Art. 19 Abs. 4 Satz 1 GG, dass ein Ausschluss des Rechtswegs nicht möglich ist. Dementsprechend verweist Art. 19 Abs. 4 Satz 3 GG auch ausschließlich auf die Ausnahme des Art. 10 Abs. 2 Satz 2 GG.

> So auch *Roggan*, DVBl 2021, 1471 (1474 f.); *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste, Verfassungsblog vom 6. Juli 2021, abrufbar unter https://verfassungsblog.de/staatstrojaner-nachrichtendienste/.

b) Beschränkte Online-Durchsuchung teilt Mängel der Quellen-Telekommunikationsüberwachung

Als Maßnahme von erheblicher Eingriffsintensität sind im Übrigen an § 11 Abs. 1a Satz 2 G 10 mindestens dieselben Anforderungen zu stellen, wie an § 11 Abs. 1a Satz 1 G 10, sodass die Vorschrift an denselben verfassungsrechtlichen Mängeln leidet.

Konkret bedeutet dies:

- Die Regelung ist bereits formell verfassungswidrig mangels einer Gesetzgebungskompetenz des Bundes. Problematisch ist in diesem Kontext nämlich nicht die fehlende Kompetenz in Bezug auf eine spezifische Maßnahme, sondern die Möglichkeit des Bundes, Ermächtigungsgrundlagen für Landesbehörden zu schaffen, die noch im Vorfeld der Gefahrenabwehr tätig sind. Eine solche Kompetenz ist weder von Art. 74 Abs. 1 Nr. 1 GG, noch Art. 73 Abs. 1 Nr. 1 oder Nr. 10 GG, noch einer anderen geschriebenen oder ungeschriebenen Kompetenznorm gedeckt (hierzu **I.2**).

- Auch in Bezug auf die beschränkte Online-Durchsuchung erlaubt § 11 Abs. 1b Satz 1 G 10 die Umgehung wesentlicher Verfahrensvorschriften durch die Erstreckung auf weitere Kennungen in verfassungswidriger Weise. Es ist nicht ersichtlich, dass in Bezug auf die beschränkte Online-Durchsuchung andere Maßstäbe angebracht wären als für die Quellen-Telekommunikationsüberwachung (hierzu **I.3.c)(1)**).

- Ebenso gehen die Einschränkungen der Benachrichtigungspflichten des § 12 Abs. 1 Satz 2 G 10 zu weit. Auch in Bezug auf den intensiven Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bedarf es aus Rechtsschutzgründen einer effektiven Benachrichtigungspflicht. Diese gewährt die vorliegende Vorschrift nicht (hierzu **I.3.c)(2)**).

- Zudem gehen die Einschränkungen durch die Eilanordnungsbefugnis des § 15a G 10 für die beschränkte Online-Durchsuchung in gleicher Weise zu weit wie für die Quellen-Telekommunikationsüberwachung (hierzu **I.3.c)(3)**).
- Da auch bei der beschränkten Online-Durchsuchung die G 10-Kommission als Kontrollorgan fungiert, sind deren Mängel auch hier zu beachten (hierzu **I.3.c)(4)**).
- Schließlich wären auch die Eingriffsvoraussetzungen unzureichend, selbst wenn auch bei der beschränkten Online-Durchsuchung modifizierte Voraussetzungen zur Anwendung kämen (hierzu **I.3.a)**).

III. Schutzpflichtverletzung (fehlendes Schwachstellenmanagement)

Durch die Ermächtigung zur Ausnutzung von Sicherheitslücken ohne gleichzeitige Einführung von Schutzvorschriften in Form eines Schwachstellenmanagements besteht zudem eine Verletzung der Schutzpflichtdimension des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.

1. Existenz einer Schutzpflicht aus dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Sinne des Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG umfasst auch die objektive Schutzpflicht des Staates, zum Schutz informationstechnischer Systeme vor Angriffen durch Dritte beizutragen. Die staatliche Schutzpflicht verlangt auch eine Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits.

> Vgl. BVerfGE 158, 170 <189 f. Rn. 44>.

Damit wird der staatliche Schutzauftrag explizit an den beschriebenen Zielkonflikt geknüpft und der großen Bedeutung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für die Funktionsfähigkeit und die Sicherheit von Staat und Gesellschaft Rechnung getragen. Somit werden die hohen, gegenwärtigen Gefahren berücksichtigt, welche die Sicherheitslücken in IT-Systemen für gewichtige Rechtsgüter für eine hohe Zahl an potenziell betroffenen Grundrechtsträgern mit sich bringen (hierzu ausführlicher **2.**).

Soweit zudem die dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG unterfallende Kommunikation ebenfalls durch die Sicherheitslücken bedroht ist, besteht auch insoweit eine staatliche Schutzpflicht.

BVerfGE 158, 170 <185 Rn. 32>.

2. Auswirkungen von Schwachstellen in informationstechnischen Systemen

Die Ausnutzung von Schwachstellen in informationstechnischen Systemen kann gravierende Folgen haben.

Aus Perspektive der IT-Sicherheit besteht ein signifikanter Unterschied zwischen Zero-Days-Schwachstellen und n-Days-Schwachstellen (hierzu bereits **B.II.**). Während die erstgenannten der Öffentlichkeit erst bekannt werden, wenn es bereits zu spät ist, können für n-Days-Schwachstellen grundsätzlich bereits technische Lösungen entwickelt worden sein. Gleichwohl zeigt sich auch hier ein sehr diverses Bild: Die Software mancher informationstechnischer Systeme, wie etwa bei Webcams oder WLAN-Router, lässt sich nicht updaten. Hier konvergieren also Zero-Days und n-Days-Schwachstellen in ihren praktischen Auswirkungen; allein eine Information aller Nutzer*innen und eine Abkoppelung der Geräte vom Internet können hier Angriffe vereiteln.

Für andere Systeme – etwa Smartphones, Laptops und Desktop-Computer – gibt es zwar prinzipiell die Möglichkeit, sowohl das Betriebssystem als auch die installierte Anwendungssoftware zu aktualisieren. Diese Möglichkeit nutzen aber sowohl die Hersteller*innen als auch die Nutzer*innen der Systeme in sehr unterschiedlicher Weise: Seitens der Hersteller*innen werden insbesondere ältere Systeme oft nicht mehr mit Updates versorgt. „Ältere“ ist hier allerdings ein sehr relativer Begriff – während beispielsweise iPhones noch einige Jahre nach dem Verkaufsschluss mit Updates des Betriebssystems iOS versorgt werden, endet die Update-Versorgung bei manchen Android-Smartphones teilweise bereits mit dem Ende des Vertriebs eines Modells oder jedenfalls wenige Monate danach.

Selbst wenn für ein bestimmtes Gerät oder eine Anwendungssoftware ein Update verfügbar wird, ist aber keineswegs gewährleistet, dass es auch jedes betroffene System (rechtzeitig) erreicht: Teilweise arbeiten Nutzer*innen jahrelang mit veralteten Versionen von Betriebssystem und Anwendungen, weil sie sich über Updates und Sicherheitslücken keine Gedanken machen oder sich von der Komplexität eines Update-Vorgangs überfordert fühlen.

Geraten n-Days-Schwachstellen, für die noch keine technischen Lösungen bestehen oder verbreitet wurden, oder Zero-Days-Schwachstellen in die falschen Hände, kann das gravierende Folgen haben (hierzu ausführlicher **a)**). So dauert es nach Kenntnis einer Sicherheitslücke im Median lediglich 22 Tage, bis eine entsprechende Schadsoftware entwickelt wird.

> *Ablon/Bogart*, Zero Days, Thousands of Nights, 2017, S. 57, abrufbar unter https://www.rand.org/pubs/research_reports/RR1751.html.

Durch die neugeschaffenen Befugnisse verschärft sich diese Gefährdungslage weiter (hierzu **b)**).

a) Gefährdungslage

Sicherheitslücken sind in alltäglichen informationstechnischen Systemen keine Ausnahme, sondern der Normalfall. Laut dem BSI ist die informationstechnische Sicherheitslage in Deutschland angespannt bis kritisch. Der Bericht zur Lage der informationstechnischen Sicherheit in Deutschland 2021 zeigt, dass die Gefahren im Cyber-Raum weiter zunehmen und auch kritische Bereiche betreffen, wie etwa die Strom- oder die medizinische Versorgung.

> Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2021, S. 3, 9; abrufbar unter https://www.bsi.bund.de/DE/ServiceNavi/Publikationen/Lagebericht/lagebericht_node.html.

Nicht nur die Anzahl von Sicherheitsvorfällen ist besorgniserregend, sondern auch die rasante Entwicklung neuer und angepasster Angriffsmethoden, die

massenhafte Ausnutzung schwerwiegender Software-Schwachstellen und die teilweise gravierenden Folgen, die erfolgreiche Cyber-Angriffe auslösen.

> Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2021, S. 4, abrufbar unter https://www.bsi.bund.de/DE/ServiceNavi/Publikationen/Lagebericht/lagebericht_node.html.

Die Verbreitung informationstechnischer Systeme in nahezu allen Lebensbereichen geht mit einer stetig steigenden Gefahr an Cyberangriffen einher, die auch über das angegriffene System hinaus Folgen nach sich ziehen. Im Jahr 2021 registrierte das BSI 144 Millionen neue Schadprogramm-Varianten, also im Durchschnitt 394.000 neue pro Tag. Die Gefahr von Cyberangriffen umgibt Nutzer*innen permanent. Allein in Regierungsnetzen wurden im Jahr 2021 74.000 Websites wegen enthaltener Schadprogramme durch den Webfilter des BSI gesperrt und 44.000 Mails mit Schadprogrammen wurden durchschnittlich pro Monat abgefangen.

> Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2021, S. 11, 43; abrufbar unter https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

Derartige Angriffe können zu erheblichen Gefahren führen, wie viele der Fälle der letzten Jahre immer wieder aufgezeigt haben.

So hat im Mai 2017 das Schadprogramm *WannaCry* weltweit Schäden verursacht, indem es die informationstechnischen Systeme von Behörden und Unternehmen, insbesondere auch von britischen Krankenhäusern lahmlegte und nur gegen Lösegeldzahlung wieder freigab. Die Sicherheitslücken, welche die hinter *WannaCry* stehenden Kriminellen ausnutzten, waren zuvor der amerikanischen NSA gestohlen worden.

> Vgl. etwa Microsoft gibt US-Regierung Mitschuld an Hackerangriff, Zeit, vom 15. Mai 2017, abrufbar unter

https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung.

Es sind keine Anhaltspunkte dafür ersichtlich, dass deutsche Nachrichtendienste Informationen über Zero-Day-Schwachstellen besser schützen könnten als die NSA.

Vgl. Cybercrime, Bundeslagebild 2021, S. 16; Google Project Zero legt Bericht zu Sicherheitslücken vor, Tagesspiegel Background vom 21. April 2022, abrufbar unter https://background.tagesspiegel.de/cybersecurity/google-project-zero-legt-bericht-zu-sicherheitsluecken-vor; Zero Day-Nutzung auf Allzeithoch, Tagesspiegel Background vom 25. April 2022 (aktualisiert am 15. Mai 2022), abrufbar unter https://background.tagesspiegel.de/cybersecurity/zero-day-nutzung-auf-allzeithoch.

Ein weiteres Beispiel ist der Ransomware-Angriff auf ein Universitätsklinikum in Nordrhein-Westfalen am 10. September 2020. Als Einfallstor für den Angriff mit den Ransomwares *DoppelPaymer* und *Dridex* nutzten die Angreifer*innen eine Schwachstelle auf dem Citrix NetScaler-Gateway des Klinikums bereits vor der Installation des zur Verfügung stehenden Sicherheitsupdates. Die Angreifer*innen hinterließen außerdem ein Erpresserschreiben. In der Folge musste sich das Krankenhaus an 13 aufeinanderfolgenden Tagen aufgrund des Ausfalls zentraler Systeme von der Notfallversorgung abmelden. Planbare und ambulante Behandlungen wurden abgesagt bzw. verschoben und die Aufnahme neuer Patient*innen wurde eingestellt. Die Kommunikation über E-Mail sowie die telefonische Erreichbarkeit des Klinikums waren eingeschränkt.

Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2021, S. 15, abrufbar unter https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

In einem ähnlichen Fall kam es im September 2020 zu einem Cyberangriff auf die informationstechnischen Systeme der Uniklinik Düsseldorf. Die Klinik sah sich gezwungen, Operationen zu verschieben und sich von der Notfallversorgung abzumelden.

> IT-Ausfall an der Uniklinik Düsseldorf, Pressemitteilung vom 17. September 2020, abrufbar unter https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/it-ausfall-an-der-uniklinik-duesseldorf.

Insbesondere werden bereits anhaltende Krisensituationen durch Cyberattacken noch weiter verstärkt. Dies zeigte nicht nur die Covid 19-Pandemie, in der Krankenhäuser bereits an ihre äußersten Kapazitäten gerieten, was durch die beschriebenen Hackerangriffe während dieses Zeitraums nur noch weiter intensiviert wurde. Auch im Zusammenhang mit dem Ukraine-Krieg werden Cyberangriffe von Russland bewusst als Mittel der Kriegsführung gegen die Ukraine, aber auch ihre Verbündeten, eingesetzt.

> Vgl. Russische Hacker greifen 42 Länder an, Tagesschau vom 23. Juni 2022, abrufbar unter https://www.tagesschau.de/ausland/europa/russland-cyber-attacken-101.html.

Überdies sind auch andere öffentliche Einrichtungen regelmäßig Opfer von Hackerangriffen. Ende April 2021 wurde etwa die Technische Universität Berlin Ziel einer schweren Cyberattacke. Bei dem Angriff hatten sich Hacker*innen Zugang zu den dezentralen Systemen der Hochschule verschafft und sich bis in die zentrale Informationstechnik vorgearbeitet. Dort erlangten sie Administratorenrechte und 5566 verschlüsselte Dateien der Universität, unter anderem vertrauliche Protokolle, Zeugnisse, Passwörter und Fotos. Verantwortlich für den Angriff war die Hackergruppe *Conti,* auf deren Blog im Darknet im Mai personenbezogene Daten von Uni-Angehörigen veröffentlicht worden waren. Die Schäden konnten teils erst nach Monaten behoben werden und allein die Wiederherstellung der aktualisierten Sicherheitsstandards in den zentralen Systemen kostete rund 445.000 Euro.

Hacker stahlen bei der TU Berlin Hunderte vertrauliche Dokumente, Berliner Zeitung vom 18. Mai 2022, abrufbar unter https://www.berliner-zeitung.de/news/hacker-stahlen-bei-der-tu-berlin-hunderte-vertrauliche-dokumente-li.228695; Keine Rückkehr zum Zustand vor dem Hackerangriff, Forschung und Lehre vom 1. September 2021, abrufbar unter https://www.forschung-und-lehre.de/forschung/keine-rueckkehr-zum-zustand-vor-dem-hackerangriff-3977.

Beispielhaft aufgeführt sei auch die schwere Cyberattacke auf das Netzwerk der Verwaltung des Landkreises Anhalt-Bitterfeld am 7. Juli 2021. Infolgedessen wurde dort der Katastrophenfall ausgerufen. Die Schadsoftware hatte die informationstechnische Infrastruktur durch Verschlüsselung lahmgelegt, woraufhin die Verwaltungstätigkeit nahezu vollständig zum Erliegen kam. Insbesondere war für mindestens eine Woche die Auszahlung von Sozial- und Unterhaltsleistungen nicht möglich. Im Zuge der Versuche, Lösegeld zu erpressen, wurden neben personenbezogenen Daten von Bürger*innen auch solche von Mandatsträger*innen im Kreistag veröffentlicht.

Hacker stellen persönliche Daten von Abgeordneten ins Darknet, Spiegel vom 6. August 2021, abrufbar unter https://www.spiegel.de/netzwelt/netzpolitik/anhalt-bitterfeld-hacker-stellen-persoenliche-daten-von-abgeordneten-ins-darknet-a-b3655f6d-0002-0001-0000-000178686047.

Auch Wirtschaftsunternehmen werden Opfer von Wirtschaftsspionage oder fremden Regierungen, häufig ohne ihr Wissen. Viele Angriffe unter Ausnutzung von Sicherheitslücken werden nicht öffentlich bekannt, weil Unternehmen nicht mit mangelnder informationstechnischer Sicherheit in Verbindung gebracht werden möchten. Aus diesem Grunde kommt zu den ohnehin hohen Fallzahlen eine hohe Dunkelziffer hinzu. Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro.

Vgl. Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, bitkom vom 5. August 2021, https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr.

Das Institut der deutschen Wirtschaft beschreibt die Cybersicherheit von Unternehmen als herausfordernd. Insbesondere durch die neuen Entwicklungen des Arbeitsalltags hin zum Homeoffice vergrößere sich durch die zunehmende Zahl an mit dem Firmennetzwerk verbundenen Systemen die Angriffsfläche. 2020 waren allein 52,5 Mrd. Euro Schaden auf Angriffe im Homeoffice zurückzuführen, 31 Mrd. Euro mehr als vor der Pandemie.

IW Kurzbericht Nr. 54, 23. August 2021, abrufbar unter: https://www.iwkoeln.de/studien/barbara-engels-525-mrd-euro-schaden-durch-angriffe-im-homeoffice-518890.html.

Nicht nur im Wirtschaftsbereich bringen Cyberattacken gewichtige Gefahren mit sich. Es ist auch die gesamte gesellschaftliche demokratische Willensbildung bedroht. So können Hackerangriffe beispielsweise auch genutzt werden, um Wahlen zu beeinflussen oder zu manipulieren und damit die gesamte Legitimation demokratisch gewählter Regierungen in Frage zu stellen.

Dies wurde im Vorfeld der US-Präsidentschaftswahl im Jahre 2016 deutlich, als durch Cyberangriffe auf E-Mail-Server im Umfeld der Präsidentschaftskandidatin Hillary Clinton sowie des Democratic National Committee Daten gestohlen und genutzt wurden, um die Wählerschaft zu beeinflussen. Einige Expert*innen vermuten, dass ausländische Geheimdienste für die Angriffe verantwortlich sind.

Hillarys schwächste Stelle, SPIEGEL vom 13. Oktober 2016, abrufbar unter https://www.spiegel.de/politik/ausland/hillary-clinton-und-der-email-hack-stecken-donald-trump-und-russland-dahinter-a-1116367.html; How the Russians hacked the DNC and passed its E-Mails to WikiLeaks, Washington Post vom 13. Juli 2018, abrufbar unter https://www.washingtonpost.com/world/national-security/how-the-

russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

Die Beispiele zeigen auf, dass sich die Gefährdungslage mit Blick auf Cyberattacken weltweit zuspitzt, und zahlreiche und bedeutende Güter von Verfassungsrang regelmäßig betroffen sind. Ein einzelner Cyberangriff geht zumeist mit der Betroffenheit einer großen Zahl an Grundrechtsträger*innen einher. Darüber hinaus beschränken sich die Auswirkungen von Cyberangriffen – wegen der Breite der Nutzung und der Abhängigkeit von Informationstechnik – nicht auf die Vertraulichkeit und Integrität des angegriffenen Systems oder die Offenbarung von personenbezogenen Daten, sondern haben das Potenzial letztlich sämtliche grundrechtlich geschützten Positionen zu gefährden.

So auch BVerfGE 158, 170 <187 Rn. 37>.

b) Verschärfung durch die neuen Überwachungsbefugnisse

Die skizzierte Gefährdungslage wird durch die neuen Überwachungsbefugnisse des § 11 Abs. 1a G 10 nur noch weiter verschärft.

Zunächst müssen die Behörden überhaupt erst Kenntnis von Sicherheitslücken erlangen, um diese im Wege der Quellen-Telekommunikationsüberwachung ausnutzen zu können. Eine Möglichkeit besteht zwar grundsätzlich darin, staatlich organisierte oder zumindest finanziell unterstützte Forschung zur Entdeckung von Zero-Day-Schwachstellen zu betreiben. Dafür könnten beispielsweise in Clouds nach neuen Möglichkeiten gesucht werden, um gefährdete Anwendungen angreifen zu können. Deutlich naheliegender ist jedoch – nicht zuletzt aufgrund mangelnder personeller Ressourcen – der Ankauf von Schwachstellen auf dem Schwarzmarkt.

Vgl. Zero-Day – Das lukrative Geschäft mit Sicherheitslücken, Tagesspiegel Background vom 9. Februar 2022, abrufbar unter https://background.tagesspiegel.de/cybersecurity/zero-day-das-lukrative-geschaeft-mit-sicherheitsluecken.

Der Ankauf dieser Lücken wird zwar nicht explizit gesetzlich ermöglicht, er wird aber auch nicht untersagt und findet in der Praxis statt.

> Vgl. bspw. Zero-Day – Das lukrative Geschäft mit Sicherheitslücken, Tagesspiegel Background vom 9. Februar 2022, abrufbar unter https://background.tagesspiegel.de/cybersecurity/zero-day-das-lukrative-geschaeft-mit-sicherheitsluecken.

Auch die unverbindliche Vorgabe im Koalitionsvertrag der aktuellen Bundesregierung „der Staat wird (daher) keine Sicherheitslücken ankaufen“,

> vgl. Mehr Fortschritt Wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), S. 87,

kann nicht darüber hinweghelfen, dass die deutschen Behörden derzeit schlicht nicht in der Lage sind, selbst Zero-Day-Schwachstellen ausfindig zu machen. Es besteht daher eine hohe Wahrscheinlichkeit, dass die Behörden auch auf den Ankauf von Sicherheitslücken ausweichen, um von der Befugnis tatsächlich Gebrauch machen zu können.

> Vgl. Zero-Day – Das lukrative Geschäft mit Sicherheitslücken, Tagesspiegel Background vom 9. Februar 2022, abrufbar unter https://background.tagesspiegel.de/cybersecurity/zero-day-das-lukrative-geschaeft-mit-sicherheitsluecken; Deutsche Behörden nutzen umstrittene Spyware, heise online vom 25. Oktober 2021, abrufbar unter https://www.heise.de/news/Deutsche-Behoerden-nutzen-umstrittene-Spyware-6221365.html; Bundesnachrichtendienst setzt Staatstrojaner Pegasus ein, netzpolitik.org vom 8. Oktober 2021, abrufbar unter https://netzpolitik.org/2021/geheimdienst-bundesnachrichtendienst-setzt-staatstrojaner-pegasus-ein/; Governments pay millions for 0days: more harm than good?, cybernews vom 16. November 2021, abrufbar unter https://cybernews.com/editorial/governments-pay-millions-for-

0days-more-harm-than-good/; The Untold History of America's Zero-Day Market, Wired vom 14. Februar 2021, https://www.wired.com/story/untold-history-americas-zero-day-market/.

Daneben besteht zwar auch grundsätzlich die Möglichkeit, dass ausländische Nachrichtendienste ihnen bekannte Sicherheitslücken mit deutschen Behörden teilen. Jedoch kaufen auch diese die Lücken in aller Regel selbst an. Zudem ist davon auszugehen, dass bei einem funktionierenden Schwachstellenmanagement eine derartige Weitergabe aus Angst der Offenlegung zumindest nur noch selten stattfinden würden.

Vgl. The NSA hacks other countries by buying millions of dollars worth of computer vulnerabilities, Washington Post vom 31. August 2013, abrufbar unter https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/.

Es sind zwar grundsätzlich noch weitere Möglichkeiten denkbar, wie der Staat entweder an Sicherheitslücken kommen könnte oder aber die Software auch ohne Sicherheitslücken auf den Systemen einspielen könnte. Diese sind aber entweder noch fernliegender oder gesetzlich nicht vorgesehen.

So wäre es grundsätzlich auch möglich, die Wohnräume der Zielpersonen zu betreten und dort manuell die Software auf vorhandenen Geräten aufzuspielen. Dieses Vorgehen ist jedoch sehr aufwändig und stellt zudem einen Eingriff in Art. 13 Abs. 1 GG dar und benötigt daher eine Ermächtigungsgrundlage, die das Artikel 10-Gesetz nicht vorsieht.

Auch wäre es zumindest in gewissen Maßen möglich, Telekommunikationsanbieter zur Mithilfe bei der Installation der Software zu ermächtigen. Dies ist aber nicht von den Mitwirkungspflichten des § 2 G 10 umfasst.

Zudem ist der Staat ein zahlungskräftiger und immer wieder auf neue Sicherheitslücken angewiesener Teilnehmer auf dem bestehenden (Schwarz-)Markt für Sicherheitslücken, welcher regelmäßig im kriminellen Milieu des Dark-

Nets stattfindet. Dies schafft und verstärkt für Expert*innen Anreize, die von ihnen entdeckten Sicherheitslücken nicht den Hersteller*innen der informationstechnischen Systeme zu melden, sondern die Schwachstellen auf dem Markt anzubieten. Zudem ist der nicht nur zahlungswillige, sondern auch zahlungsfähige „Stammkunde Staat“ ein verlockender Geschäftspartner, da von ihm keine Gefahr der Strafverfolgung ausgeht. Folglich ist zu erwarten, dass eine solche Teilnahme des Staates am (Schwarz-)Markt für Sicherheitslücken nicht zur Sicherheit informationstechnischer Systeme beiträgt, sondern die Gefährdungslage vielmehr weiter verschärfen wird.

> Zero-Day – Das lukrative Geschäft mit Sicherheitslücken Tagesspiegel Background vom 9. Februar 2022, abrufbar unter https://background.tagesspiegel.de/cybersecurity/zero-day-das-lukrative-geschaeft-mit-sicherheitsluecken.

Sind die Sicherheitslücken den Behörden schließlich bekannt, werden diese darüber hinaus geheim gehalten, um die Schwachstellen zum eigenen Interesse ausnutzen zu können. Dadurch wird den Hersteller*innen der Systeme die Möglichkeit verwehrt, eine entdeckte Sicherheitslücke mithilfe ihrer spezifischen Fachexpertise schnellstmöglich zu schließen. Je länger die Sicherheitslücke geheim gehalten wird, desto höher ist dabei die Gefahr eines Missbrauchs durch kriminelle Dritte für folgenschwere Hackerangriffe. Die Geheimhaltung von Sicherheitslücken wurde beispielsweise bereits durch das das BKA bestätigt.

> Das BKA verhindert, dass Sicherheitslücken geschlossen werden, Netzpolitik.org vom 12. November 2018, abrufbar unter https://netzpolitik.org/2018/it-sicherheit-das-bka-verhindert-dass-sicherheitsluecken-geschlossen-werden/.

Schließlich kommt belastend hinzu, dass der Staat zunächst eine gewisse Einarbeitungszeit benötigt, um die Sicherheitslücke auch für die Quellen-Telekommunikationsüberwachung nutzen zu können. Dadurch wird ein zusätzlicher Anreiz geschaffen, die jeweilige Schwachstelle möglichst lang geheim zu halten.

3. Verletzung der staatlichen Schutzpflicht

Die Maßnahmen des § 11 Abs. 1a G 10 liegen im Spannungsfeld von informationstechnischer Sicherheit und Verfassungsschutz. Neben die klassische abwehrrechtliche Dimension des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme tritt eine Schutzpflichtdimension, die den Staat grundsätzlich dazu verpflichtet, zur Sicherheit der IT-Infrastruktur beizutragen und Systeme vor Zugriffen und Manipulationen Dritter zu schützen.

Deshalb ist ein gesetzliches Schwachstellenmanagement erforderlich, welches regelt, unter welchen Bedingungen Hersteller*innen Sicherheitslücken zu melden sind (hierzu **a)**). Dem genügen die vorhandenen Regelungen allerdings bisher nicht einmal im Ansatz (hierzu **b)**). Hierdurch wird die aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG folgende grundrechtliche Schutzpflicht verletzt.

a) Verfassungsrechtlicher Maßstab

Nach dem angerufenen Gericht umfasst das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auch eine Schutzpflichtdimension.

> Vgl. BVerfGE 158, 170 <184 f. Rn. 26 ff.>.

Grundsätzlich steht dem Gesetzgeber nach der Rechtsprechung des angerufenen Gerichts bei der Erfüllung derartiger grundrechtlicher Schutzpflichten ein weiter Einschätzungs-, Wertungs- und Gestaltungsspielraum zu. Dieser an der Effektivität des Grundrechtsschutzes ausgerichtete Spielraum kann sich hinsichtlich des Umfangs und Form der Regelung verengen, je nachdem, welcher Sachbereich und welche Rechtsgüter betroffen sind.

> Vgl. BVerfG, Beschluss vom 16. Dezember 2021 – 1 BvR 1541/20, Rn. 99.

Darüber hinaus gebietet es die Wesentlichkeitstheorie, welche sich aus dem grundlegenden Demokratie- und Rechtsstaatsprinzip ableiten lässt, dass der Gesetzgeber es nicht der Exekutive überlassen darf, wesentliche Entscheidungen mit hoher Grundrechtsrelevanz zu treffen, sondern diese selbst im Wege eines Parlamentsgesetzes zu regeln hat.

Vgl. BVerfGE 41, 251 <259 f.>; 45, 400 <417 f.>.

Nach der Rechtsprechung des angerufenen Gerichts gebietet gerade die Schutzpflicht des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eine Beschränkung des gesetzgeberischen Spielraums. So verlangt die Schutzpflicht eine Regelung darüber, wie eine Behörde bei der Entscheidung über ein Offenhalten unerkannter Sicherheitslücken den Zielkonflikt zwischen dem notwendigen Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung von Quellen-Telekommunikationsüberwachungen andererseits aufzulösen hat. Der Behörde muss eine Abwägung der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine Zero-Day-Schutzlücke bekannt wird. Es ist sicherzustellen, dass die Behörde bei jeder Entscheidung über ein Offenhalten einer unbekannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt, beides zueinander ins Verhältnis setzt und die Sicherheitslücke an Hersteller*innen meldet, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt.

Vgl. BVerfGE 158, 170 <189 f. Rn. 44>.

Unter Berücksichtigung der unüberschaubaren Zahl an betroffenen Grundrechtsträger*innen und besonders bedeutsamen Rechtsgütern, ist die Entscheidung über die Ausgestaltung eines Schwachstellenmanagements von so wesentlicher Bedeutung, dass diese einer konkreten parlamentsgesetzlichen Form bedarf. Mithin kann diese Entscheidung nicht allgemeinen und deshalb zwangsläufig in ihrem Gehalt unbestimmteren Regelungen überlassen werden. Vielmehr müssen die Vorschriften dem Gebot der Normenklarheit und

Bestimmtheit entsprechen und sowohl den Belangen der einzelnen betroffenen Person als auch dem objektiv-rechtlich geschützten kollektiven Interesse an einem hinreichend hohen Standard der IT-Sicherheit Rechnung tragen.

Auch darüber hinaus ergeben sich aus der jüngeren Entscheidungspraxis des angerufenen Gerichts hohe Anforderungen im Bereich des Sicherheitsrechts, die auch im Rahmen der hier zur Diskussion stehenden Schutzpflicht von Relevanz sind.

So hat das angerufene Gericht in seinem Urteil zur *Vorratsdatenspeicherung* ausgeführt, dass der Gesetzgeber für die bevorrateten Daten einen „besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben“ muss.

BVerfGE 125, 260 <327>.

Die Sicherheit der Vorratsdaten hat ähnlich wie das hier in Rede stehende Schwachstellenmanagement sowohl eine individuelle, auf die einzelne betroffene Person bezogene, als auch eine kollektive, auf die Gesamtheit der bevorrateten Daten bezogene Dimension. Das angerufene Gericht hat verlangt, dass die maßgeblichen Gesichtspunkte spezifisch für die Vorratsdatenspeicherung geregelt werden. Die stets zu erfüllende allgemeine Verpflichtung der Telekommunikationsdienste-Anbieter zum Schutz des Fernmeldegeheimnisses hat das angerufene Gericht für nicht ausreichend gehalten, um den gebotenen Schutzstandard zu gewährleisten, obwohl eine entsprechend strenge Auslegung der maßgeblichen Regelungen *lege artis* durchaus möglich gewesen wäre.

Vgl. BVerfGE 125, 260 <348 ff.>.

In seinem Urteil zur *Antiterrordatei* hat das angerufene Gericht beanstandet, dass das Gesetz keine ausdrückliche Verpflichtung der Datenschutzaufsichtsbehörden zu turnusmäßigen Kontrollen der Datei enthielt.

BVerfGE 133, 277 <371>.

Eine solch regelmäßige Kontrolle, die nicht an bestimmte Ereignisse oder Verdachtsmomente anknüpft, dient neben dem Schutz konkreter betroffener Personen gerade auch dem kollektiven Interesse an einer effektiven Durchsetzung des Datenschutzrechts. Eine Pflicht zu turnusmäßigen Kontrollen hätte sich im Fall der *Antiterrordatei* wiederum durchaus aus den gesetzlichen Regelungen über die Kontrollaufgaben der Datenschutzaufsicht im Wege einer verfassungsgeleiteten Reduktion des Kontrollermessens herleiten lassen. Gleichwohl hat das angerufene Gericht auch hier eine spezifische und ausdrückliche gesetzliche Vorgabe verlangt.

Schließlich hat das angerufene Gericht in seinen Urteilen zur *Antiterrordatei* und zum *BKA-Gesetz* im Zusammenhang mit eingriffsintensiven Überwachungsmaßnahmen regelmäßige Berichtspflichten gegenüber Parlament und Öffentlichkeit eingefordert, damit eine öffentliche Diskussion über diese Maßnahmen ermöglicht und diese einer demokratischen Kontrolle und Überprüfung unterworfen werden.

> BVerfGE 133, 277 <372>; 141, 220 <285>.

Die Berichtspflichten dienen besonders deutlich gerade auch kollektiven, objektiv-verfassungsrechtlichen Belangen, die jedoch untrennbar mit den grundrechtlichen Abwehrrechten verknüpft sind. Auch hier hätte sich eine turnusmäßig zu erfüllende Rechenschaftspflicht durchaus auf der Grundlage einer verfassungsgeleiteten Interpretation allgemeiner parlamentsrechtlicher Vorgaben entwickeln lassen. Hingegen hat das angerufene Gericht eine ausdrückliche und maßnahmespezifische gesetzliche Regelung für erforderlich gehalten.

Schließlich hat das angerufene Gericht in seinen Urteilen zur *Ausland-Ausland-Fernmeldeaufklärung* und zum *Bayerischen Verfassungsschutzgesetz* hervorgehoben, dass besonders grundrechtsensible Entscheidungen auch im geheimdienstlichen Bereich nur auf Grundlage hinreichend normenklarer und bestimmter Rechtsgrundlagen gefällt werden dürfen.

Vgl. BVerfGE 154, 152 <238 f.>, BVerfG, Urteil vom 26.4.2022 – 1 BvR 1619/17, Rn. 272 f.

Maßgebend in Bezug auf die Bestimmtheit ist, dass das Gesetz gerade dort für die handelnde Behörde „steuernde und begrenzende Handlungsmaßstäbe“ vorsieht, wo aufgrund des Geheimhaltungsbedürfnisses eine Konkretisierung „im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle“ des Regelungsgehalts nur unzureichend erfolgt. Der Grundsatz der Normenklarheit begrenzt wiederum die Zulässigkeit gesetzlicher Verweisungsketten auf ein Maß, das die Regelungen in Aussagegehalt und Anwendungstauglichkeit nicht übermäßig schmälert.

Dabei verlangte das Gericht in der letztgenannten Entscheidung auch, dass bereits durch den Gesetzgeber bestimmt und normenklar eingriffsangemessene Stufen der Beobachtungsbedürftigkeit von Bestrebungen und Aktionen festgelegt werden. Eine Bestimmung allein durch die Behörde ist nicht ausreichend, auch wenn diese ihrerseits an den Verhältnismäßigkeitsgrundsatz gebunden ist und damit bereits aus diesem Grund die Beobachtungsbedürftigkeit bei der Entscheidung zu berücksichtigen hat, ob eine eingriffsintensive Maßnahme ergriffen wird.

Vgl. BVerfG, Urteil vom 26.4.2022 – 1 BvR 1619/17, Rn. 203 f.

Die jüngere Rechtsprechung des angerufenen Gerichts zum Sicherheitsrecht zeigt damit eine deutliche Tendenz, für objektiv-verfassungsrechtliche Vorgaben, die in spezifischer Weise mit subjektiven Eingriffsabwehrrechten verwoben sind, eine problemspezifische, normenklare und bestimmte gesetzliche Ausgestaltung zu verlangen. Über die gängigen Grundsätze der Schutzpflichtendogmatik geht diese Rechtsprechung deutlich hinaus.

Schließlich ist zu berücksichtigen, dass konkrete Einzelheiten des Schwachstellenmanagements zwangsläufig geheim gehalten werden müssen. Eine öffentliche Bekanntgabe der Risikoeinschätzungen und Schlussfolgerungen der Überwachungsbehörde würde den Betroffenen ermöglichen, sich auf die für sie bestehenden Risiken einzustellen und gegebenenfalls Gegenmaßnahmen

zu ergreifen (etwa die Nutzung nur bestimmter Betriebssysteme oder Kommunikationssoftware).

b) Fehlen erforderlicher Schutzmechanismen

Die vorgenannten Anforderungen wurden durch den Gesetzgeber mangels eines Schwachstellenmanagements schon im Ansatz nicht erfüllt. Ein derartiges Regelungssystem lässt sich selbst im Rahmen einer extensiven und verfassungskonformen Interpretation den bisher vorhandenen Normen nicht entnehmen.

Es bestehen keine spezifischen Regelungen für den Zielkonflikt (hierzu **(1)**). Darüber hinaus sind auch die Vorschriften zur Datenschutz-Folgeabschätzung (hierzu **(2)**), die Regelungen zum BSI (hierzu **(3)**) und die sonstige IT-Sicherheitsarchitektur des Bundes (hierzu **(4)**) unzureichend. Auch außerhalb formeller Bundesgesetze sind derartige Schutzregelungen nicht zu finden. So ergibt sich ein Schutzmanagement weder aus dem Europa- und Völkerrecht (hierzu **(5)**) noch aus landesrechtlichen Regelungen (hierzu **(6)**) und auch nicht aus untergesetzlichen Regelungen (hierzu **(7)**). Insgesamt ergibt sich ein Bild, wonach auch durch das Zusammenspiel der vorhandenen Regelungen kein hinreichendes Schutzniveau erreicht wird (hierzu **(8)**).

(1) Keine spezifische Schutzregelung für den Zielkonflikt

Es besteht keine spezifische Schutzregelung, um den Zielkonflikt zu adressieren. Insbesondere besteht keine Rechtsgrundlage für ein behördliches Schwachstellenmanagement. § 11 Abs. 1a Satz 4 und Satz 5 G 10 enthalten zwar Sicherungsklauseln, beide betreffen aber nicht Sicherheitslücken. Auch im Rahmen einer extensiven Auslegung kann den Vorschriften eine derartige Bedeutung nicht entnommen werden. Auch darüber hinaus enthält das Artikel 10-Gesetz keine Regelung zu einem Schwachstellenmanagement.

(a) § 11 Abs. 1a Satz 4 G 10 enthält keine Regelung zu einem Schwachstellenmanagement

§ 11 Abs. 1a Satz 4 G 10 – nachdem das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen ist – scheidet als Grundlage für ein behördliches Schwachstellenmanagement evident aus. Keine der Auslegungsmethoden Wortlaut (hierzu **(i)**), Systematik (hierzu **(ii)**), Entstehungsgeschichte (hierzu **(iii)**) oder Telos der Vorschrift (hierzu **(iv)**) ergeben auch nur Anhaltspunkte für ein Schwachstellenmanagement. Eine extensive, vom Leitgedanken der Schutzpflicht getragene Auslegung kann daher zu keinem anderen Ergebnis kommen (hierzu **(v)**).

Siehe auch *Roggan*, DVBl 2021, 1471 (1473).

(i) Wortlaut des § 11 Abs. 1a Satz 4 G 10

Bereits der Wortlaut von § 11 Abs. 1a Satz 4 G 10 beschränkt die Vorschrift eindeutig auf die eingesetzte Software. Die Vorschrift bezieht sich auf das eingesetzte Mittel. Als Mittel werden gemeinhin Handlungen oder Gegenstände bezeichnet, die zielgerichtet eingesetzt werden, um einen Zweck zu erreichen. Mittel zeichnen sich dadurch aus, dass die handelnde Person sie in einem Mindestmaß beherrscht und auf den Einsatzzweck zurichtet.

Von Mitteln abzugrenzen sind Gegenstände, auf die sich eine zweckgerichtete Handlung bezieht, also die Objekte dieser Handlung. Bei der beschränkten Online-Durchsuchung und Quellen-Telekommunikationsüberwachung gilt: Das Mittel zur Durchführung dieser Maßnahmen ist die eingesetzte Software. Diese nutzt lediglich eine Sicherheitslücke aus.

Darüber hinaus ordnet § 11 Abs. 1a Satz 4 G 10 ausdrücklich an, das eingesetzte Mittel „nach dem Stand der Technik“ abzusichern. Diese Anordnung ergibt nur Sinn, soweit sie auf die Überwachungssoftware bezogen wird. Sie verlangt, bei der Gestaltung der Software anerkannte Maßstäbe der IT-Sicherheit zu beachten. Die Behörde hat aber überhaupt nicht die Möglichkeit, die Sicherheitslücke nach dem Stand der Technik zu schützen. Stand der Technik im Umgang mit Sicherheitslücken ist, durch Nachbesserungen von Hard- oder

Software solche Lücken zu schließen oder zumindest ihre Ausnutzung zu erschweren. Gerade das soll aber nicht geschehen, wenn eine beschränkte Online-Durchsuchung oder Quellen-Telekommunikationsüberwachung unter Ausnutzung einer Schwachstelle durchgeführt wird. Vielmehr würde die Sicherung der Schwachstelle nicht nur den Zugriff durch Dritte, sondern auch den Zugriff der Behörde beenden, was dem angestrebten Ziel zuwiderlaufen würde.

Auch kontrolliert die Behörde das System nicht und kann daher auch selbst keine Sicherheitslücken schließen. Dies kann ausschließlich durch die Hersteller*innen geschehen.

Aus behördlicher Sicht wäre eine Schwachstelle aber nicht nach dem Stand der Technik zu schließen, sondern im Rahmen eines Abwägungs- und Meldeverfahrens.

Durch den Zusatz „nach dem Stand der Technik“ weicht die Vorschrift auch im erheblichen Maße von der Vorschrift des § 54 Abs. 3 Satz 2 Baden-Württembergischen Polizeigesetzes ab, dessen unzureichende Analyse das erkennende Gericht in einem anderen Verfahren anmahnte.

> BVerfGE 158, 170 <192 Rn. 54 f.>.

Bereits bei der angesprochenen landesrechtlichen Norm ist äußerst zweifelhaft, ob diese einer verfassungsgeleiteten Auslegung zugänglich ist, nach welcher die Norm auch Vorgaben zu einem Schwachstellenmanagement enthält. Durch den Zusatz „nach dem Stand der Technik“ ist eine solche Deutung für § 11 Abs. 1a Satz 4 G 10 aber ausgeschlossen.

(ii) Systematik des § 11 Abs. 1a Satz 4 G 10

Auch die Systematik der Vorschrift enthält keinerlei Hinweise, darauf, dass der Vorschrift ein Schwachstellenmanagement entnommen werden könnte. Innerhalb des § 11 G 10 schreibt § 11 Abs. 1a Satz 6 G 10 eine Protokollierungspflicht für jeden Einsatz des Mittels vor. Demnach sind nach Satz 6 Nr. 3 Angaben zu protokollieren, „die die Feststellung der erhobenen Daten ermöglichen“. Bei der Schließung einer Sicherheitslücke werden jedoch keinerlei

Daten erhoben, vielmehr erfolgt eine Veränderung des informationstechnischen Systems. Folglich geht der Gesetzgeber selbst davon aus, dass der Einsatz technischer Mittel sich auf die Erhebung von Daten bezieht, nicht auf das Verhindern der Erhebung von Daten durch die Schließung von Sicherheitslücken.

Auch im systematischen Vergleich außerhalb des Artikel 10-Gesetzes mit der Parallelnorm § 100a Abs. 1 Satz 2 und 3 sowie § 100 Abs. 5 und 6 StPO ergibt sich kein anderes Ergebnis. § 11 Abs. 1a Satz 4 G 10 ist nach dem Willen des Gesetzgebers an die strafprozessuale Norm und diese wiederum an § 49 Abs. 2 Satz 2 BKAG angelehnt.

> BT-Drs. 19/24785, S. 22, BT-Drs. 18/12785, S. 53.

Diesbezüglich entspricht es den gesetzgeberischen Erwägungen und der herrschenden Auffassung im Schrifttum, dass die mit § 11 Abs. 1a Satz 4 G 10 wortgleiche Regelung der §§ 49 Abs. 2 Satz 2 BKAG, 100a Abs. 5 Satz 2 StPO ausschließlich Bestimmungen zur Gestaltung und Sicherung der verwendeten Überwachungssoftware treffen.

> Vgl. zu § 49 BKAG: BT-Drs. 16/10121, S. 29; zu § 100a StPO: *Köhler*, in: Meyer-Goßner/Schmitt, 63. Aufl. 2020, § 100a Rn. 14i; *Bruns*, in: KK-StPO, 8. Aufl. 2019, § 100a Rn. 45, § 100a Rn. 92; *Eschelbach*, in: Satzger/Schluckebier/Widmaier, StPO, 4. Aufl. 2020, § 100a Rn. 47; *Graf*, in: BeckOK StPO, Stand 2022, § 100a Rn. 135, § 100a Rn. 141; *Freiling/Safferling/Rückert*, JR 2018, 9 (12); *Hauck*, in: LR-StPO, 27. Aufl. 2019, § 100a Rn. 158.

Ebenso wie § 11 Abs. 1a G 10 hat die Regelung in § 100a Abs. 5 StPO Kritik wegen fehlender Vorgaben zum Umgang mit Schwachstellen hervorgerufen.

> Siehe *Bruns*, in: KK-StPO, 8. Aufl. 2019, § 100a Rn. 46; vgl. ferner *Eschelbach*, in: Satzger/Schluckebier/Widmaier, StPO, 5. Aufl. 2020, § 100a Rn. 45; *Derin/Golla*, NJW 2019, 1111.

(iii) Historischer Hintergrund des § 11 Abs. 1a Satz 4 G 10

Auch aus der Gesetzeshistorie des § 100a StPO lassen sich keine Anhaltspunkte für ein Schwachstellenmanagement ableiten. Trotz Kritik an einem fehlendem Schwachstellenmanagement während des Gesetzgebungsprozesses wurde dieses unverändert verabschiedet.

> Vgl. *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, BT Ausschuss-Drs. 19(4)844 A, S. 7 ff.; *Poscher*, Stellungnahme zu dem Entwurf der Bundesregierung eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Mai 2021, BT Ausschuss-Drs. 19(4)844 E, S. 10 f.; BT-Plenarprotokoll 19/233, S. 29980; *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, BT Ausschuss-Drs. 18(6)334, S. 20 ff.; *Neumann*, Sachverständigenauskunft zum Änderungsantrag der Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, BT-Ausschuss-Drs. 18/11272, S. 5 ff; siehe auch *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste, Verfassungsblog vom 6. Juli 2021, abrufbar unter https://verfassungsblog.de/staatstrojaner-nachrichtendienste/

Der Gesetzgeber hätte in Kenntnis der vorhandenen Kritik sowie der Auslegung von § 100 Abs. 5 StPO reagieren können und den Wortlaut der Vorschrift ergänzen oder anpassen können. Da er dies unterlassen hat, kann nur davon ausgegangen werden, dass die Norm gerade kein Schwachstellenmanagement enthalten soll.

(iv) Sinn und Zweck des § 11 Abs. 1a Satz 4 G 10

Schließlich ergibt sich auch nichts anderes aus dem Sinn und Zweck der Verpflichtung nach § 11 Abs. 1a G 10, das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Die Vorschrift dient einerseits dazu, dass die eingesetzte Software nicht von Dritten zu normwidrigen Zwe-

cken ausgenutzt werden kann. Andererseits sichert die Verpflichtung die weitere Durchführbarkeit von Maßnahmen nach § 11 Abs. 1a G 10.

Würde sich die Schutzvorgabe auch auf Zero-Day-Schwachstellen beziehen, wäre eine weitere Nutzung der Infiltrationssoftware und damit eine fortgesetzte Durchführung der Überwachungsmaßnahme aber schlicht nicht möglich. Entweder wird die Schwachstelle gemeldet und in der Folge geschlossen oder diese wird nicht gemeldet und bleibt bestehen. Da für die Schließung der Schwachstelle die Hersteller*innen der entsprechenden IT-Systeme verantwortlich sind, erscheint es abwegig, dass nach Meldung eine Lücke nur für Dritte geschlossen wird, den Nachrichtendiensten aber weiterhin offensteht.

Der Norm können auch keine Vorgaben dazu entnommen werden, nur unter bestimmten Umständen eine Schwachstelle zu melden, da sie derartige Einschränkungen gerade nicht enthält. Dem klaren Wortlaut nach wäre bei einer folgerichtigen Subsumtion stets eine Meldung zu erstatten, da nur so ein effektiver Schutz gegen eine unbefugte Nutzung gewährleistet werden könnte.

Selbst wenn es – unter Missachtung der obigen Auslegungsversuche – der Zweck der Norm wäre, das *Wissen* um die Sicherheitslücke „nach dem Stand der Technik“ gegen Kenntnisnahme durch Dritte zu schützen, würde das nicht einem Schwachstellenmanagement entsprechen. Denn ein solches Schwachstellenmanagement würde sich gerade nicht in der bloßen Sicherung des Wissens um die Sicherheitslücke erschöpfen, sondern müsste – am Ende eines Abwägungsprozesses – auch zu dem Ergebnis kommen können, dass die Sicherheitslücke den Hersteller*innen zu melden ist.

(v) Keine extensive Auslegung des § 11 Abs. 1a Satz 4 G 10 möglich

Letztlich bestehen auch keine Anknüpfungspunkte, um die Vorschrift im Wege einer verfassungsgeleiteten, extensiven Auslegung um ein Schwachstellenmanagement zu ergänzen. Denn eine solche ist nur möglich, wenn sich im Gesamtzusammenhang der Vorschrift Anknüpfungspunkte für verfassungsrechtliche Wertungen ergeben.

> BVerfGE 138, 64 <93 f. Rn. 86>.

Dies ist vorliegend jedoch gerade nicht der Fall. Stattdessen würde das Hineinlesen eines Schwachstellenmanagements in § 11 Abs. 1a Satz 4 G 10 den normativen Grundgehalt der Norm grundlegend neu bestimmen. Doch gerade im Bereich verfassungsrechtlicher Schutzpflichten ist eine derartige „verfassungskonforme Rechtsfortbildung“ nicht zulässig.

Voßkuhle, AöR 2000, 177 (197 f.).

Eine Interpretation, nach der die Vorschrift lediglich die Meldung von Schwachstellen ermöglichen würde, könnte wiederum nicht zur Erfüllung der staatlichen Schutzpflichten führen. Denn eine derartige Möglichkeit allein ist nicht ausreichend, um ein hinreichendes Schwachstellenmanagement darzustellen. Durch die Quellen-Telekommunikationsüberwachung und beschränkte Online-Durchsuchung wird ein Anreiz geschaffen, Sicherheitslücken möglichst lang aufrecht zu erhalten. Besteht lediglich die gesetzliche Möglichkeit, diese zu melden, ist in nicht ausreichender Form sichergestellt, dass es zu solchen Meldungen kommt. Dass Behörden im Rahmen einer Ermessensentscheidung über eine derartige Meldung die Grundrechte zu berücksichtigen haben, reicht nicht aus. Vielmehr müsste aufgrund der hohen Grundrechtsrelevanz bereits durch den Gesetzgeber vorgegeben sein, unter welchen Voraussetzungen eine Meldung zu erfolgen hat. Die entsprechenden Normen müssen den Anforderungen an die Normenklarheit und Bestimmtheit genügen (hierzu bereits **a)**).

Vgl. BVerfGE 141, 220 <265 Rn. 94 > m.w.N.

Dies ist bei § 11 Abs. 1a Satz 4 G 10 evident nicht der Fall. Die Vorschrift adressiert weder den genannten Zielkonflikt noch nennt sie konkrete Abwägungskriterien.

(b) § 11 Abs. 1a Satz 5 G 10 unzureichend

Nach § 11 Abs. 1a Satz 5 G 10 sind „kopierte Daten nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.“ Die Norm schützt allgemein die Sicherung der aus dem System

erhobenen Daten. In § 11 Abs. 1a Satz 5 G 10 ist mithin nicht geregelt, wie mit dem Bekanntwerden einer Sicherheitslücke umzugehen und wie der beschriebene Zielkonflikt aufzulösen ist. Vielmehr schützt § 11 Abs. 1a Satz 5 G 10 die bereits kopierten Daten vor dem Zugriff unbefugter Dritter, nicht jedoch die Schwachstelle selbst. Mithin ist auch in § 11 Abs. 1a Satz 5 G 10 kein Schwachstellenmanagement geregelt.

(c) Auch darüber hinaus keine Regelungen zum Schwachstellenmanagement im Artikel 10-Gesetz enthalten

Auch wenn damit Vorschriften bestehen, die einige der Gefahren durch den Einsatz neuartiger Software minimieren sollen, enthalten diese keine Regelung zum Umgang mit Sicherheitslücken im Sinne eines Schwachstellenmanagements. Auch darüber hinaus enthält das Artikel 10-Gesetz keine Vorschriften, denen ein Schwachstellenmanagement entnommen werden könnte.

(2) Datenschutz-Folgeabschätzungsregelungen unzureichend

Auch § 67 BDSG und entsprechenden landesrechtlichen Normen zur Datenschutz-Folgeabschätzung sind keine Vorgaben zu einem Schwachstellenmanagement zu entnehmen. Die Norm ist bereits nicht auf Nachrichtendienste anwendbar (hierzu **(a)**). Der aufgezeigte Zielkonflikt ist zudem nicht vom Tatbestand der Norm erfasst und kann auch durch richtlinienkonforme Auslegung nicht im Sinne eines Schwachstellenmanagements interpretiert werden (hierzu **(b)**). Jedenfalls aber ergeben sich auch aus § 67 BDSG keine den bestimmten und normenklaren Regelungen zum Schwachstellenmanagement (hierzu **(c)**) erfüllen.

(a) Keine normenklare Geltung der Datenschutz-Folgeabschätzung für die Nachrichtendienste

Das gefundene Auslegungsergebnis wird gestützt durch die bloß eingeschränkte Anwendbarkeit des § 67 BDSG für die in § 1 Abs. 1 G 10 adressierten Behörden. Aufgrund der erheblichen Grundrechtsrelevanz bedarf es nor-

menklarer Regelungen zur Umsetzung der staatlichen Schutzpflicht. Eine Vorschrift, die nicht unmittelbar für die maßgeblichen Behörden gilt und anwendbar ist, kann diese Anforderungen nicht erfüllen.

> Vgl. BVerfG, Urteil vom 26.4.2022 – 1 BvR 1619/17, Rn. 272 f.

Die gesetzlichen Grundlagen auf Bundesebene enthalten nur eingeschränkte Verweise auf das BDSG (§ 27 Nr. 2 BVerfSchG; § 64 Nr.2 BND-G; § 13 Nr. 2 MADG). Die Datenschutz-Folgeabschätzung ist von den Verweisungen nicht umfasst.

Auch auf die Landesverfassungsschutzbehörden findet die Vorschrift nur im Ausnahmefall Anwendung. Nach § 1 Abs. 1 Nr. 2 BDSG ist dies nur der Fall, soweit der Datenschutz nicht durch Landesgesetz normiert wird. Auf die Landesgesetzgebung zum Datenschutz hat der Bund wiederum keinen Einfluss. Ein Überblick über den Regelungsbestand in

> Art. 14 BayDSG, § 53 BlnDSG, § 62 HDSIG, § 39 NDSG, § 56 DSG NRW, §§ 9, 56 LDSG RhPf, § 23 SächsDSUG, § 14 SaarlDSG, § 43 LDSG SH und § 52 ThürDSG

zeigt, dass zwar viele, aber nicht alle Bundesländer eine Datenschutz-Folgeabschätzung normiert haben. Die Landesverfassungsschutzgesetze, konkret

> § 18 LVSG, Art. 28 BayVSG, § 38 VSG Bln, § 27 BbgVerfSchG, 31 Brem-VerfSchG, 23c HmBVerfSchG, § 30 LVerfSchG M-V, § 33b NVerfSchG, § 31 VSG NRW, § 39 LVerfSchG RhPf, § 19 SächsVSG, § 30 VerfSchG-LSA und 36 ThürVerfSchG,

enthalten indes ebenfalls nur eingeschränkte Verweise auf die jeweiligen Landesdatenschutzgesetz sowie das BDSG.

(b) Keine tatbestandliche Anwendbarkeit des § 67 BDSG auf das Offenhalten von Schwachstellen

Mit Blick auf die Tatbestandsvoraussetzungen ist festzustellen, dass das Offenhalten von IT-Sicherheitslücken bei unterstellter Anwendbarkeit keine Verpflichtung des jeweiligen Nachrichtendienstes zur Datenschutz-Folgeabwägung auslösen kann und das Schwachstellenmanagement somit nicht vom Tatbestand des § 67 BDSG erfasst ist.

Dies gilt zunächst im Hinblick auf das Tatbestandsmerkmal des „Verarbeitungsvorgangs". Die gesetzgeberischen Erwägungen stellen heraus, dass unter „Verarbeitungsvorgang" nicht die einzelne Verarbeitung zu verstehen sei, sondern ohne erheblichen Mehraufwand „lediglich die Verwendung maßgeblicher Systeme und Verfahren zur Verarbeitung personenbezogener Daten mithilfe einer Datenschutz-Folgeabschätzung vorab in den Blick genommen werden" muss.

> BT Drs. 18/11325, S. 117.

Diese Zielrichtung findet im Wortlaut der Norm ihren Niederschlag, wonach eine Verarbeitung „insbesondere bei der Verwendung neuer Technologien" einer Folgeabschätzung zu unterziehen ist. Zudem spricht ein systematischer Vergleich mit der Parallelnorm § 69 Abs. 1 S.1 Nr. 1 BDSG dafür, dass sich die Verpflichtung weniger auf die Einzelverarbeitung, als die übergeordnete Entscheidung über die Verwendung (neuer) Verarbeitungssysteme und Verfahren sowie deren wesentliche Veränderung bezieht.

> Vgl. *Thiel,* in: Gola/Heckmann, 13. Aufl. 2019, § 69 BDSG Rn. 2; S. 42, *Nolden,* in: Paal/Pauly, 3. Aufl. 2021, § 69 BDSG Rn. 3.

Die Entscheidung über das Offenhalten einer konkreten Sicherheitslücke liegt aber zeitlich nach der generellen Entscheidung über den Einsatz der Quellen-TKÜ als technischer Infiltrationsmaßnahme und stellt sich damit allenfalls als Vorbereitungsmaßnahme eines konkreten, nicht der Folgeabschätzung unterliegenden Einzelzugriffs nach dem Artikel 10-Gesetz dar. Weder der Ankauf von Sicherheitslücken noch das Offenhalten in Form eines unterbleibenden

Hinweises an Hersteller*innen stellen einen „Verarbeitungsvorgang“ im Sinne der Norm dar.

Überdies gehen vom generellen Einsatz der Quellen-Telekommunikationsüberwachung, wie auch von der konkreten Maßnahme selbst keine „Folgen“ im Sinne des § 67 Abs. 1 BDSG für die IT-Sicherheit aus. Die qualitative Erhöhung der Gefahr eines unberechtigten Fremdzugriffs resultiert erst aus der fortwährenden Untätigkeit staatlicher Behörden nach Kenntniserlangung von Sicherheitslücken.

Auch das tatbestandliche Anknüpfen an die Maßnahmen des § 11 Abs. 1a G 10 führt zu keinem Schwachstellenmanagement. Die Gefahren für die IT-Sicherheit insgesamt gehen nicht von einzelnen Quellen-Telekommunikationsüberwachungen und beschränkten Online-Durchsuchungen aus, sondern von den Handlungen im Vorfeld oder im Nachgang dieser Überwachungsmaßnahmen.

Auch eine europarechtskonforme Auslegung kann nicht zu einem anderen Ergebnis führen. Zwar beruht § 67 BDSG auf Art. 27 RL (EU) 2016/680 vom 27. April 2016 (JI-RL). Allerdings ist bereits die Anwendbarkeit der Richtlinie im nachrichtendienstlichen Kontext fraglich.

> Vgl. *Bäcker,* in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, S. 65; *Weichert,* Die EU-Richtlinie für den Datenschutz bei Polizei und Justiz, Netzwerk Datenschutzexpertise vom 1. Februar 2016, S.12, abrufbar unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/bewertung_2016_02_eudsri_polizei.pdf.

Die Richtlinie erfasst nicht die Tätigkeit von Stellen, die mit Fragen der nationalen Sicherheit befasst sind.

> Vgl. JI-RL, Erwägungsgrund 14.

Auch nach Art. 2 Abs. 2 lit. a DSGVO und Art. 2 Abs. 3 lit. a JI-RL finden diese Regelungswerke keine Anwendung auf Datenverarbeitungen im Rahmen von

Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen. Die Nachrichtendienste dürfen beschränkte Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen allein zur Aufklärung schwerwiegender Gefährdungslagen für die nationale Sicherheit einsetzen (§ 3 Abs. 1 G 10), für deren Schutz gemäß Art. 4 Abs. 2 Satz 3 EUV ausschließlich die Mitgliedstaaten zuständig sind. Die Behörden agieren insoweit im Kernbereich des nachrichtendienstlichen Aufklärungsauftrags, für den allgemein anerkannt ist, dass der Anwendungsbereich des europäischen Datenschutzrechts nicht eröffnet ist.

> Vgl. *Zerdick*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 2 Rn. 8; *Bäcker*, in: BeckOK Datenschutzrecht, Stand November 2021, DSGVO, Art. 2 Rn. 9d; *Geiger*, in: Jäger/Daun, Geheimdienste in Europa – Transformation, Kooperation und Kontrolle, 1. Aufl. 2009, S. 243 f.

Auch darüber hinaus würde eine Berücksichtigung von Art. 27 JI-RL zu keinem anderen Ergebnis führen. Während § 67 BDSG lediglich an „eine erhebliche Gefahr für die Rechtsgüter betroffener Personen“ anknüpft, geht die Richtlinie darüber hinaus, sodass zu berücksichtigen ist, ob „ein hohes Risiko für Rechte und Freiheiten natürlicher Personen“ entsteht. Auch wenn damit also ein anderer Maßstab zugrunde zu legen ist, ändert das nichts daran, wann eine Datenschutz-Folgenabschätzung überhaupt zum Einsatz kommt. Auch die Richtlinie knüpft hierbei an eine Verarbeitung an. Eine Verarbeitung ist in Art. 3 Nr. 2 der Richtlinie definiert als „jede[r] mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“. Nichts davon kann auch nur annähernd dahingehend ausgelegt werden, dass es auch das Vorbereitungsstadium einer Datenverarbeitung erfassen könnte, in dem aber die Entscheidung über die Offenlegung von Sicherheitslücken

getroffen wird. Auch das fortdauernde Unterlassen der Offenlegung einer solchen Sicherheitslücke stellt keine Verarbeitung im Sinn der Vorschrift dar.

Einer erweiternden, richtlinienkonformen Auslegung auf die Auflösung des Zielkonfliktes steht zudem entgegen, dass auch die Parallelnormen Art. 27 JI-RL und Art. 35 EU-DSGVO die Datenschutz-Folgeabschätzung systematisch nicht als Rechtmäßigkeitsvoraussetzung der Datenverarbeitung einbetten, sondern lediglich die allgemeine Rechenschaftspflicht des Verantwortlichen (vgl. Art. 4 Abs. 4 JI-RL, Art. 5 Abs. 2 EU-DSGVO) als Verfahrensregel konkretisieren.

Vgl. BSG, Urteil vom 20.1.2021 – B 1 KR 7/20 R, Rn. 84 m.w.N.

Die Datenschutz-Folgeabschätzung eignet sich folglich nicht, die verfassungsrechtlich bedeutsame Auflösung des Zielkonfliktes durch die Nachrichtendienste zu regeln.

(c) Keine hinreichend bestimmte Regelung des Zielkonflikts durch § 67 BDSG

Schließlich würde § 67 BDSG aufgrund seiner geringen Regelungsdichte selbst bei tatbestandlicher und uneingeschränkter Anwendbarkeit nicht den aus dem Gebot der Bestimmtheit folgenden Anforderungen an eine einfachgesetzliche Konkretisierung der staatlichen Schutzpflicht genügen.

Zwar ordnet § 67 BDSG eine Abwägung der entgegenstehenden Belange an. Eine hinreichende Regelung des Schwachstellenmanagements erfordert jedoch eine konkretere Bestimmung, nicht lediglich eine schlichte Abwägungsregel. So bedarf es bestimmter Vorgaben zur Auflösung des Zielkonflikts zwischen dem einzelfallbezogenen Anliegen einer wirksamen nachrichtendienstlichen Aufklärung und dem allgemeinen Erfordernis eines möglichst hohen Niveaus der IT-Sicherheit in Deutschland. In diesem Sinne fehlt es § 67 BDSG sowohl an eindeutigen Vorgaben für den Umgang mit hohen Risiken (siehe hierzu die restriktivere Parallelnorm Art. 35 EU-DSGVO), als auch an Rechtsfolgeregelungen, die sicherstellen, dass Sicherheitslücken zwingend an Her-

steller*innen gemeldet wird, soweit das nachrichtendienstliche Interesse an der Offenhaltung der Lücke nicht überwiegt.

(3) Regelungen zum BSI ungenügend

Grundsätzlich sieht die gesetzgeberische Konzeption mit dem BSI eine Behörde vor, welche die Aufgabe und Befugnis hat, Sicherheitslücken zu offenbaren (§ 7 Abs. 1 Satz 1 Nr. 2 lit. a, b BSIG i.V.m. § 3 Abs. 1 Satz 2 Nr. 14, 14a BSIG). Das BSI kann seinen gesetzlichen Auftrag indes nur erfüllen, soweit diesem auch Erkenntnisse zu Sicherheitslücken vorliegen. Die bestehenden Regelungen stellen nicht sicher, dass das BSI seinen Pflichten nachkommen kann. Bereits die Grundkonzeption des Regelfalls zur Offenbarung von Sicherheitslücken durch das BSI genügt nicht, um den gesetzgeberischen Schutzauftrag zu erfüllen (hierzu **(a)**). Hinzukommt, dass von diesem unzulänglichem Regelungskomplex weitreichende Ausnahmetatbestände bestehen (hierzu **(b)**).

(a) Regelfall beim BSI

Prinzipiell korrespondieren mit der vorbezeichneten Aufgabenzuweisung Meldepflichten anderer Behörden und privater Dritter. Dies gilt zunächst nach dem BSIG für Bundesbehörden gemäß § 4 Abs. 3 i.V.m. Abs. 2 Nr. 1 BSIG, Betreiber Kritischer Infrastrukturen (KRITIS) gemäß § 8b Abs. 3, 4 BSIG und Anbieter digitaler Dienste gemäß § 8c Abs. 3, 4 BSIG.

Auch Landesbehörden sind nach §§ 2, 3 des Beschlusses 2017/35 des IT-Planungsrates i.V.m. § 2 Abs. 1, 2 Satz 2 des Vertrags über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (IT-Staatsvertrag) – zur Meldung im Rahmen des VerwaltungsCERT-Verbund (VCV) und damit auch gegenüber dem Computer Emergency Response Team (CERT) des Bundes beim BSI meldepflichtig.

Auf EU-Ebene sehen Art. 14 Abs. 5 und Art. 16 Abs. 6 der RL (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnah-

men zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL) einen Informationszufluss von Seiten der IT-Sicherheitsbehörden anderer EU-Mitgliedsstaaten vor.

Problematisch ist jedoch bereits, dass eine potenziell meldepflichtige Sicherheitslücke für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sein muss (§ 4 Abs. 3 BSIG). Diese entscheidende Einschätzung im Vorfeld einer potenziellen Mitteilung nimmt die berichtspflichtige Behörde selbst vor. Entsprechend müssen Bundes- und Landesbehörden die Möglichkeit der Auswirkung des Sicherheitsvorfalls auf Bund und Länder oder dessen Relevanz für Bund und Länder zunächst einmal erkennen (§ 4 Abs. 3 BSIG, § 2 Abs. 1 des Beschlusses 2017/35 des IT-Planungsrates). Eine solche Vorverlagerung der Beurteilung von IT-Sicherheitslücken auf – nicht zwingend fachkundige – Stellen birgt die Gefahr, dass das BSI bereits nicht in die Lage versetzt wird, die Bedeutung für seine Aufgabenwahrnehmung selbst beurteilen zu können. Eine nachträgliche, gegebenenfalls stichprobenartige Überprüfung nicht gemeldeter Vorfälle durch das BSI ist nicht vorgesehen, es existieren keine flankierenden Kontrollmechanismen.

Hinzu kommt, dass die potenziell meldepflichtige Stelle nur die Bedeutung der Sicherheitslücke für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden beurteilen muss, nicht aber die Bedeutung für die Allgemeinheit. Das Prüfprogramm ist also unzureichend.

Darüber hinaus ist nach Mitteilung von Sicherheitslücken an das BSI nicht sichergestellt, dass diese ordnungsgemäß bewertet und an Hersteller*innen gemeldet werden. Insbesondere stellt § 5 der vom Bundesministerium des Innern und für Heimat (BMI) erlassenen Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Abs. 6 BSIG keine Kriterien auf, nach denen eine Sicherheitslücke zu bewerten ist.

Schließlich ist dem BSI nach § 7 Abs. 1 Satz 1, Nr. 1 lit. a, b, Satz 2 BSIG ein von konkreten Vorgaben befreiter Ermessensspielraum eingeräumt, ob es schlussendlich eine Warnung ausspricht oder nicht.

Schulte, in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes, 1. Aufl. 2021, § 7 Rn. 307.

Der Gesetzgeber kann sich an dieser Stelle nicht auf eine schutzpflichtgeleitete Auslegung oder Ermessensreduktion auf null in Einzelfällen verlassen. Vielmehr obliegt es ihm, selbst bereits normenklar und bestimmt darzulegen, wann eine Sicherheitslücke zu offenbaren ist und wann diese verschwiegen und damit offengehalten werden kann (hierzu bereits **a)**).

(b) Ausnahmen vom Regelfall

Neben diesen Unzulänglichkeiten des Regelfalls ist zusätzlich davon auszugehen, dass das BSI nach dem bestehenden Regelungsgefüge regelmäßig überhaupt erst gar keine Informationen über die von den Nachrichtendiensten verwendeten Sicherheitslücken erlangt, diese folglich auch gar nicht offenbaren kann.

Die Zulässigkeit der Übermittlung und Weitergabe von Informationen durch die Nachrichtendienste des Bundes an das BSI richtet sich nämlich nicht nach dem BSIG, sondern allein nach den für diese geltenden Vorschriften. In diesen nachrichtendienstlichen Gesetzen zu Übermittlungspflichten sind allerdings weitreichende Ausnahmen enthalten. § 4 Abs. 4 BSIG nimmt jene Informationen von der Übermittlung aus, die aufgrund von Regelungen zum Geheimschutz (hierzu **(i)**) oder Vereinbarungen mit Dritten (hierzu **(ii)**) nicht weitergegeben werden dürfen.

(i) Geheimschutz als Ausnahmetatbestand

Unter die Regelungen zum Geheimnisschutz fallen – wie § 4 Abs. 6 BSIG i.V.m. § 2 Abs. 3 der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gem. § 4 Abs. 6 BSIG konkretisiert – sämtliche Informationen, deren Weitergabe nach den maßgeblichen Regelungen im BVerfSchG, BNDG und MADG untersagt ist.

Vgl. Gesetzesbegründung zu § 4 Abs. 4 BSIG BT-Drs. 16/11967, S. 13.

Insoweit maßgeblich ist folglich das Übermittlungsverbot in § 23 BVerfSchG, welches im Bereich des BND und des MAD über Verweisungsnormen Anwendung findet (§ 18 BNDG, § 12 MADG).

Dabei ist bereits bezeichnend, dass die Vorschriften des § 23 BVerfSchG sich streng genommen überhaupt nicht auf Übermittlungen gegenüber dem BSI beziehen („Übermittlungen nach den Vorschriften dieses Abschnitts"). Das zeigt deutlich auf, dass sich der Gesetzgeber zum konkreten Verhältnis zwischen den Nachrichtendiensten und dem BSI bereits generell keine Gedanken gemacht und insbesondere kein spezifisches Schwachstellenmanagement vorgesehen hat.

§ 23 BVerfSchG stellt sich nicht als verfassungskonforme Konkretisierung der objektiven Schutzpflicht dar. Die Regelung hält kein hinreichendes Konzept zum Umgang mit Zero-Day-Schwachstellen vor. Weder lassen sich dem Gesetz klare Kriterien zur Abwägung zwischen Offenlegung und Geheimhaltung entnehmen (hierzu **(aa)**) noch enthält der Regelungszusammenhang ein den verfassungsrechtlichen Anforderungen genügendes System, welches eine effektive Kontrolle der nachrichtendienstlichen Entscheidung ermöglicht (hierzu **(bb)**). Daran hat auch das IT-Sicherheitsgesetz 2.0 vom 18. Mai 2021 (BGBl. I 2021, S. 1122) nichts geändert, das die Systematik der die Nachrichtendienste betreffenden Meldepflichten und Ausnahmen unangetastet gelassen hat.

(aa) Keine Vorgaben zur Abwägung des Zielkonflikts im Kontext des Übermittlungsverbotes

Nach § 23 Nr. 2 BVerfSchG kann eine Meldung unterbleiben, wenn „überwiegende Sicherheitsinteressen dies erfordern". Der Vorschrift ist keine Abwägung des erwähnten Zielkonflikts zu entnehmen, vielmehr besteht die Norm seit der Verkündung des Bundesverfassungsschutzgesetzes von 1990 unverändert fort. Es ist davon auszugehen, dass die Nachrichtendienste eine unterbleibende Übermittlung regelmäßig auf diesen Ausnahmetatbestand stützen dürften, da keine klaren Maßstäbe für die Auslegung bestehen.

Aus einem systematischen Vergleich mit entsprechenden landesrechtlichen Regelungen (Art. 27 Nr. 2 BayVSG, § 23 Abs. 1 Nr. 2 HVSG sowie § 27 Nr. 2 LVerfSchG RhPf) lässt sich entnehmen, dass unter Sicherheitsinteressen nicht etwa auch IT-Sicherheitsinteressen der Allgemeinheit, sondern allein die Interessen des jeweiligen Nachrichtendienstes zu verstehen sind. Die vorbezeichneten Normen zeigen, dass schutzwürdige Interessen insbesondere im Schutz von Quellen, Nachrichtenzugängen und operativen Maßnahmen zu erkennen sind. Wenn bekannt gewordene IT-Sicherheitslücken für eigene Zwecke nutzbar gemacht werden sollen, wird dem jeweiligen Nachrichtendienst ein weiter Spielraum zugebilligt. Die Behörde wird sich regelmäßig im Namen der Funktionsfähigkeit nachrichtendienstlicher Aufklärung zugunsten der Geheimhaltung entscheiden und sich so der Übermittlungspflicht nach § 4 Abs. 3 BSIG entziehen. So kommt es entgegen der grundsätzlichen Konzeption des BSI als zentrale Melde- und Informationsstelle zu einer Verschiebung der Sachentscheidungskompetenz, die an sich nicht durch die bloße Vorschrift zur Datenübermittlung gedeckt ist.

> Vgl. *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 1. Aufl. 2002, S. 324; *Bergemann*, in: Lisken/Denninger, PolR-HdB, 7. Aufl. 2021, H. Nachrichtendienste und Polizei, Rn. 142 f.; *Poscher/Rusteberg*, in: Dietrich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 1. Aufl. 2019, S.155 m.w.N, 158.

Dabei wird nicht verkannt, dass § 23 Nr. 2 BVerfSchG seinem Wortlaut nach grundsätzlich eine Abwägung mit gegenläufigen Interessen wie der Effektivität der Gefahrenabwehr sowie grundrechtlich geschützten Individualinteressen erfordert. Gleichwohl bleibt die Entscheidung des jeweiligen Nachrichtendienstes losgelöst von konkreten gesetzlichen Vorgaben, anhand derer die Interessenabwägung zur Auflösung des Zielkonflikts zu erfolgen hat – unter Verstoß gegen das Vorbehaltsprinzip.

> Vgl. BVerfGE 158, 170, <189 Rn. 44>.

Gerade dort, wo wegen der Geheimschutzinteressen eine Konkretisierung der unbestimmten Regelung im Wechselspiel mit einer unabhängigen Instanz nicht erfolgt, steht der Gesetzgeber in der Verantwortung, normenklar und bestimmt steuernde und begrenzende Handlungsmaßstäbe festzulegen, die die behördliche Entscheidung leiten.

Die Konsequenz der fehlenden gesetzlichen Konkretisierung zeigt sich darin, dass zugunsten der Nachrichtendienste ein Sicherheitsinteresse im Regelfall als gegeben angenommen wird und zum Schutz nachrichtendienstlicher Quellen und Arbeitsmethoden in der Regel von einem zu schützenden Sicherheitsinteresse ausgegangen werden kann.

> Vgl. *Bock*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG, § 23 Rn. 6, 7, 10.

Ein teilweise vertretener Rückgriff auf sich aus strafrechtlichen Vorschriften wie § 138 StGB ergebenden Orientierungshilfen, würde ebenfalls keinen weitergehenden Schutz informationstechnischer Systeme bewirken.

> Vgl. *Bock*, in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG, § 23 Rn. 8.

Denn deren Normappell richtet sich weder an die Behörde anstelle des Individuums noch enthält der Katalog typische Delikte (§§ 202a ff. StGB), die mit dem Ausnutzen von IT-Sicherheitslücken verwirklicht werden. In der Konsequenz besteht das erhebliche Risiko einer unangemessenen Gewichtung nachrichtendienstlicher Interessen, welche sich bereits in der Vergangenheit etwa im Rahmen des NSU-Komplexes am Beispiel des Quellenschutzes zu einer nahezu absoluten Übervorteilung verdichtet haben.

> Vgl. BT-Drs. 17/14600, S. 217; Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus vom 30. April 2013, S. 359.

Die in der Aufarbeitung des NSU-Komplexes durch die Regierungskommission zur Überprüfung der Sicherheitsgesetze in Deutschland empfohlene Anpas-

sung des § 23 BVerfSchG fand nichtsdestotrotz keine Umsetzung auf Bundesebene.

> *Pichl,* Untersuchung im Rechtsstaat – Eine deskriptiv-kritische Beobachtung der parlamentarischen Untersuchungsausschüsse zur NSU-Mordserie, 1. Aufl. 2022, S. 298*;* vgl. auch Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetze in Deutschland vom 28. August 2013, S. 204, 275.

Somit wird auch aus der Entstehungsgeschichte deutlich, dass unter Sicherheitsinteressen die Interessen des jeweiligen Nachrichtendienstes zu verstehen sind. Lediglich in einigen Bundesländern (Art. 27 Abs. 2 BayVSG, § 19 Abs. 2 BbG VerfSchG, § 23 HSVG) kam es zu einer an der Empfehlung orientierten Änderung von Übermittlungsverboten, die jedoch ebenso wenig auf die Auflösung des Zielkonfliktes im Umgang mit IT-Sicherheitslücken ausgerichtet sind.

Fachgerichtliche Rechtsprechung zu dieser Frage existiert nicht und ist – mangels der Möglichkeit, gegen eine (nicht bekannte) Unterlassung von Meldungen vorzugehen – auch nicht zu erwarten. Das angerufene Gericht hat sich zu § 23 Nr. 2 BVerfSchG in seinem Urteil zur *Auslands-Auslands-Fernmeldeaufklärung* nicht geäußert. Es hat allein mit Blick auf § 23 Nr. 1 BVerfSchG erklärt, dass dieses Übermittlungsverbot mit seinem sehr offenen Auslegungsansatz nicht geeignet ist, eine hinreichend normenklare Regelung, die verfassungsrechtlich geboten ist, zu ersetzen.

> BVerfGE 154, 152 <307>.

Mangels konkreter Regelungen liegt es nahe, dass die Nachrichtendienste sich bei der Beurteilung, wann „überwiegende Sicherheitsinteressen“ bestehen, einseitig von den eigenen Interessen leiten lassen und im Regelfall der Geheimhaltung den Vorzug geben. Allein ein auf demokratische Weise legitimiertes, hinreichend spezifisches Normprogramm, welches Abwägungskriterien für die Entscheidung über den Zielkonflikt festlegt, kann dieser Vorfestlegung der Nachrichtendienste mit ausreichender Sicherheit entgegenwirken.

(bb) Keine hinreichenden Kontroll- und Aufsichtsregelungen

Die mangelhaften Vorgaben zur Entscheidungsfindung werden durch ein Zuständigkeits-, Aufsichts- und Kontrollsystem flankiert, welches die nachrichtendienstrechtliche Absenkung der üblichen rechtsstaatlichen Sicherungen nicht zu kompensieren vermag.

So liegt es allein in der Hand des jeweiligen Nachrichtendienstes, darüber zu befinden, ob eine Sicherheitslücke wegen überwiegender Sicherheitsinteressen dem BSI nicht übermittelt wird. Interne oder externe unabhängige Kontrollgremien, die von der Entscheidung über den Umgang mit einer bekannt gewordenen Schwachstelle unverzüglich zu unterrichten wären oder denen gegenüber sogar die Entscheidung im Sinne einer Förderung der Selbstkontrolle zu begründen wäre, sind gesetzlich nicht vorgesehen.

Das objektiv-rechtliche Kontrollvakuum zur Einhaltung der Übermittlungspflichten und -verbote wird auch weder durch Kontrollrechte des PKGr nach § 14 G 10 noch durch solche der nach § 15 G 10 eingerichteten G 10-Kommission gefüllt. Denn die Abwägungsentscheidung über das Offenhalten einer bekannten Sicherheitslücke stellt keine Beschränkungsmaßnahme nach dem G 10-Gesetz im Sinne von § 14 Abs. 1 Satz 2 und § 15 Abs. 5 und 6 G 10 dar, sondern ist dem späteren konkret-individuellen Einsatz in zeitlich unbestimmtem Umfang vorgelagert.

Zudem ist die Berichtspflicht des BMI gegenüber dem PKGr mit ihren großzügigen zeitlichen Intervallen von bis zu sechs Monaten ungeeignet, die unverzügliche Auflösung der Kollision der Schutzgüter effektiv zu überwachen. Auch die monatliche Unterrichtungspflicht des BMI gegenüber der G 10-Kommision gem. § 15 Abs. 7 G 10 über erfolgte oder unterbliebene Mitteilungen, welche jedoch ihrem klaren Wortlaut nach nicht auf innerbehördliche Übermittlungen, sondern allein auf die Benachrichtigung von Betroffenen nach § 12 G 10 über erfolgte Beschränkungsmaßnahme bezogen ist, ist als Kontrollmaßnahme bezüglich des Umgangs mit Sicherheitslücken ungeeignet.

Des Weiteren wird keine effektive Überprüfung durch die zum 1. Januar 2022 erfolgte Einrichtung des Unabhängigen Kontrollrats mit dem Gesetz zur Ände-

rung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts (BGBl. I S. 2274) gewährleistet. Abgesehen von dem Umstand, dass dieser nach § 42 BNDG lediglich Tätigkeiten des BND und nicht der übrigen Nachrichtendienste vorab kontrolliert, bezieht sich die Kontrolle nicht auf den Umgang mit Sicherheitslücken, sondern die Anordnung von Maßnahmen in der strategischen Fernmelde- und Telekommunikationsüberwachung im Ausland.

Schließlich weist § 28 Abs. 2 Satz 1 BVerfSchG dem*r Bundesbeauftragten für Datenschutz lediglich die Kontrollbefugnis für die Einhaltung von Datenschutzvorschriften zu. Das Offenhalten von Schwachstellen stellt sich aber nicht als Datenverarbeitung und damit als unmittelbar datenschutzrelevanter Vorgang dar (hierzu bereits ausführlich **(2)(b)**). Dementsprechend besteht auch insoweit keine unabhängige Kontrolle der Abwägungsentscheidung.

(ii) Drittvereinbarungen als Ausnahmetatbestand

Schließlich erfahren die der Meldepflicht unterliegenden Tatbestände zu IT-Schwachstellen nach § 4 Abs. 4 Var. 2 BSIG eine weitere erhebliche Einschränkung. Selbst wenn unterstellt würde, dass ein Nachrichtendienst im Rahmen einer Abwägung die eigenen Sicherheitsinteressen im Sinne von § 23 Nr. 2 BVerfSchG nicht für überwiegend erachte, so liefe die Meldepflicht gem. § 4 Abs. 3 BSIG in Bezug auf die hier relevanten Sicherheitslücken aufgrund von Vereinbarungen mit Dritten regelmäßig leer.

Gerade die für den Eingriff nach § 11 Abs. 1a G 10 bedeutsamen Zero-Day-Sicherheitslücken können oftmals nur durch Ankauf auf dem Schwarzmarkt oder informelle Weitergabe von ausländischen Nachrichtendiensten in Erfahrung gebracht werden.

> Vgl. The NSA hacks other countries by buying millions of dollars worth of computer vulnerabilities, Washington Post vom 31. August 2013, abrufbar unter https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/; BND will In-

formationen über Software-Sicherheitslücken einkaufen, Spiegel vom 9. November 2014, abrufbar unter https://www.spiegel.de/politik/deutschland/bnd-will-informationen-ueber-software-sicherheitsluecken-einkaufen-a-1001844.html; Zero-Day – Das lukrative Geschäft mit Sicherheitslücken, Tagesspiegel Background vom 9. Februar 2022, abrufbar unter https://background.tagesspiegel.de/cybersecurity/zero-day-das-lukrative-geschaeft-mit-sicherheitsluecken.

Dabei haben sämtliche Akteure ein gewichtiges Interesse daran, dass die geteilten Sicherheitslücken nicht geschlossen werden. In der internationalen nachrichtendienstlichen Kooperation beruht der Umgang mit Informationen auf der sog. *Third Party Rule.* Diese bildet nach dem angerufenen Gericht eine für die Wahrung der sicherheitspolitischen Interessen der Bundesrepublik besonders bedeutsame, „auf Vereinbarungen mit Partnerdiensten beruhende allgemein anerkannte Verhaltensregel unter Nachrichtendiensten, nach der Informationen von ausländischen Diensten nach Maßgabe informeller Absprachen nicht ohne deren Zustimmung weitergegeben werden dürfen".

BVerfGE 154, 152 <297 f.>.

§ 4 Abs. 4 BSIG normiert allerdings keine inhaltlichen Anforderungen an derartige Vertraulichkeitsvereinbarungen der Nachrichtendienste. So räumt der Gesetzgeber den Nachrichtendiensten des Bundes nicht nur die Möglichkeit ein, sich auf Vertraulichkeitsvereinbarungen jeder Art berufen zu können – ohne dass diese Entscheidung einer unabhängigen Kontrolle unterworfen wäre –, sondern schafft mittelbar auch einen Anreiz, Sicherheitslücken überhaupt erst von Dritten zu beziehen, um somit eine Weitergabe von Informationen ohne weitergehende Abwägung zu versagen.

Zudem kann bei Existenz einer derartigen Vorschrift gar kein effektives Schwachstellenmanagement vorliegen. Gerade beim so problematischen Ankauf von Zero-Days-Sicherheitslücken wird es immer zu Vertraulichkeitsvereinbarungen kommen. Damit wird aber die vom Gericht geforderte Abwägung

der gegenseitigen Interessen bereits kategorisch zu Gunsten der Geheimhaltung entschieden.

Vgl. zu den Anforderungen BVerfGE 158, 170 <189 f. Rn. 44>.

Auch eine verfassungskonforme Reduktion der Vorschrift, kann die verfassungsrechtlichen Mängel der Vorschrift nicht gänzlich beseitigen. Ebenso wie im Rahmen des § 23 Nr. 2 BVerfSchG fehlt es an der notwendigen hinreichend bestimmten, normenklaren gesetzgeberischen Regelung, die die Missbrauchsgefahren der pauschalen Berufung auf Drittvereinbarungen bannt und einer insgesamt verfassungskonformen Praxis im Umgang mit Schwachstellen zuführt. Vielmehr muss der Gesetzgeber bestimmte Anforderungen an die Geheimhaltungsvereinbarungen mit Dritten stellen, die beispielsweise die Höchstdauer des Geheimnisschutzes festlegen oder einen Abschluss bei erheblichen Gefährdungen generell untersagen.

Ergänzend sei darauf hingewiesen, dass die *Third Party Rule* einer solchen gesetzlichen Regelung nicht entgegenstehen kann. Deren Beachtung darf nach der Rechtsprechung des angerufenen Gerichts nicht mit einem vollumfänglichen Ausschluss von steuernden Kontrollmechanismen einhergehen.

BVerfGE 154, 152 <296 ff.>.

(4) Sonstige IT-Sicherheitsarchitektur des Bundes unzulänglich

Der Bund genügt seiner staatlichen Schutzpflicht zur Aufdeckung von IT-Sicherheitslücken auch nicht durch eine Vielzahl an insbesondere in den letzten Jahren geschaffenen unterschiedlichen Stellen, die im weitesten Sinne mit IT-Sicherheit befasst sind.

Vgl. *Kreutzer/Schneider,* DuD 2021, S. 249 (250 ff.).

Hierzu gehören beispielsweise die Agentur für Innovation in der Cybersicherheit GmbH, die Bundesagentur für Sprunginnovationen, die Bundesakademie für Sicherheitspolitik, das Cyber Innovation Hub, Deutschland sicher im Netz e.V., das Forschungsinstitut Cyber Defense, das Forschungsrahmenprogramm

der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“, die Kompetenz- und Forschungszentren für IT-Sicherheit CISPA, ATHENE und KASTEL, die Stiftung Wissenschaft und Politik, die Allianz für CyberSicherheit des BSI, das Bündnis für Cybersicherheit, das Bundes Security Operations Center, die CERT-Verbünde, das Cybersicherheitsnetzwerk, die Föderale IT-Kooperation, das Gemeinsame Lagezentrum Cyber- und Informationsraum, das Informationstechnikzentrum Bund, der IT-Planungsrat, der Nationale CyberSicherheitsrat, der Nationale Pakt Cybersicherheit, das Nationale Cyber-Abwehrzentrum, das Nationale IT-Lagezentrum, die Transferstelle IT-Sicherheit im Mittelstand und die Zentrale Stelle für Informationstechnik im Sicherheitsbereich.

Obgleich der staatlichen Beratungs- und Forschungspolitik und der Koordination von IT-Sicherheitsbehörden eine bedeutende Rolle im Zusammenhang mit der Erfüllung objektiver Schutzpflichten im IT-Bereich zukommt, können diese die aufgezeigten Lücken im Schwachstellenmanagement nicht kompensieren.

Denn nach dem Willen des Gesetzgebers kommt dem BSI die wesentliche Aufgabe zu, als zentrale Stelle sämtliche Meldungen über Sicherheitsvorfälle zu bündeln und das weitere Vorgehen festzulegen. Solange das BSI aber von einem Hauptteil des Informationszuflusses – nämlich vonseiten der Nachrichtendienste – im Regelfall abgeschnitten bleibt, behält das im Übrigen bestehende Erforschungs-, Melde- und Informationssystem fragmentarischen Charakter.

Selbst wenn es nicht ausgeschlossen erscheint, dass sich der Anteil von durch zivile bzw. nicht-nachrichtendienstliche Einrichtungen entdeckten Sicherheitslücken dank der staatlichen Maßnahmen künftig steigert, vermögen diese nicht diejenigen abwägungsbezogenen Defizite des Gesamtkonzepts zum Umgang mit Zero-Days-Schwachstellen auszugleichen, welche die gesetzliche Ermächtigung zum Einsatz der Quellen-Telekommunikationsüberwachung durch die Nachrichtendienste zur Entstehung gelangen lässt. Der entstandene Zielkonflikt muss vielmehr vom Gesetzgeber selbst geregelt werden.

Zudem lässt sich auch bezweifeln, dass die Vielzahl an Institutionen wirklich zu einer Verbesserung der IT-Sicherheit führt. Vielmehr ist zu befürchten, dass ein immer undurchsichtigeres Netz an Zuständigkeiten in diesem Bereich die Arbeit der Stellen sogar noch erschwert.

(5) Unzureichende Regelungen auf europa- und völkerrechtlicher Ebene

Es ist bereits zweifelhaft, ob sich der Bundesgesetzgeber durch einen Verweis auf europa- bzw. völkerrechtliche Rechtsetzungsakte seiner eigenen Schutzpflicht entledigen kann. Jedenfalls bestehen aber auch auf diesen Ebenen keine Regelungen, an denen sich ein Schwachstellenmanagement auf nationaler Ebene ausrichten ließe.

Es fehlt bereits an einer europarechtlichen Kompetenz im Bereich der nationalen Nachrichtendienste. Diese verbleibt im Rahmen der Kompetenz für nationale Sicherheit gemäß Art. 4 Abs. 2 Satz 3 EUV bei den Mitgliedstaaten. Sofern Regelungen zur IT-Sicherheit existieren, entfalten diese dementsprechend auch keine unmittelbare Wirkung auf die entsprechenden Behörden (hierzu bereits **(2)(b)**).

Der bestehenden EU-Agentur für Netz- und Informationssicherheit (ENISA) – kürzlich gestärkt durch eine Erweiterung der Betätigungsfelder auf Grundlage des EU Cybersecurity Act (VO (EU) 881/2019 vom 17. April 2019) – kommt lediglich eine koordinierende und beratende Funktion zu. Angesichts der zudem bislang allenfalls ansatzweise etablierten europäischen Meldesysteme (Art. 14 Abs. 5, Art. 16 Abs. 6 NiS-RL) können im Vergleich zum BSI-Regelungskomplex auf EU-Ebene keine Normen ausgemacht werden, welche die Ausrichtung eines nationalen Schwachstellenmanagements bestimmen könnten.

Dies zeigt sich nicht zuletzt daran, dass der Entwurf der Europäischen Kommission zur NiS-Richtlinie 2.0 (COM(2020) 823 final, 2020/0359 (COD)) in Art. 6 überhaupt erst den Aufbau eines europäischen Schwachstellenregisters

durch ENISA sowie die Beteiligung der nationalen CSIRTs (= Computer Security Incident Response Team) an einer europaweit koordinierten Offenlegung von Schwachstellen (Art. 10 Abs. 2 lit. f) anstrebt.

Im Völkerrecht bestehen ebenfalls keine zwingenden Vorschriften, welche die deutschen Nachrichtendienste zur Veröffentlichung von Schwachstellen informationstechnischer Systeme verpflichten oder instruktiv zum Schwachstellenmanagement herangezogen werden könnten.

(6) Landesgesetze ungenügend

Auch in Bezug auf Landesgesetze ist fraglich, ob sich der Bund überhaupt auf diese hinsichtlich der Erfüllung einer eigenen Schutzpflicht berufen könnte.

Wenn der Bund überhaupt über eine Regelungskompetenz verfügen würde, die es ihm ermöglichen würde, auch die Landesverfassungsschutzbehörden zum Einsatz der Quellen-Telekommunikationsüberwachung und der beschränkten Online-Durchsuchung zu ermächtigen, so müsste er dann auch eine umfassende Regelung treffen. Konsequenterweise würde dies auch ein effektives Schwachstellenmanagement umfassen, um der grundrechtlichen Regelungsverantwortung zu genügen.

Ginge man von einer Möglichkeit der Erfüllung des grundrechtlichen Schutzauftrags durch Landesgesetze aus, ist diesbezüglich bereits problematisch, dass der Bund eine Änderung der entsprechenden Regelungssysteme weder verhindern noch beeinflussen könnte. Jedenfalls besteht aber auch unter Berücksichtigung der Landesebene kein hinreichendes Schwachstellenmanagement.

Zunächst können diese die Nachrichtendienste des Bundes als Bundesbehörden nicht verpflichten. Allenfalls die daneben ermächtigten Landesämter für Verfassungsschutz könnten somit einem landesrechtlich ausgeformten Schwachstellenmanagement unterliegen.

Indes besteht selbst auf Landesebene kein einheitliches Regulierungsbild, welches auf die Existenz eines auch bundesweiten Schwachstellenmanage-

ments schließen lassen könnte. Selbst wenn einzelne Vorschriften, wie etwa Art. 27 Abs. 2 BayVSG, § 19 Abs. 2 BbG VerfSchG, § 23 HSVG und – mit Abstrichen – § 22 Abs. 2 ThürVerfSchG, im Ansatz weitergehende Anforderungen an die Abwägung zwischen nachrichtendienstlichen und gefahrenabwehrbezogenen Belangen stellen, wollten die jeweiligen Landesgesetzgeber hierdurch keine Verpflichtung einzelner Landesämter zur Aufdeckung von IT-Sicherheitslücken normieren. Die Vorschriften richten sich vielmehr nach der Empfehlung der Regierungskommission zur Aufarbeitung des NSU-Komplexes aus, um die Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten zu stärken.

> Vgl. BayLT-Drs. 17/11609, S. 24; HessLT-Dr. 19/5412, S. 51; Bbg-LT-Drs. 6/10948, S. 24; Thür-LT-Drs. 5/8080 S 955 f.

Die übrigen länderrechtlichen Übermittlungsverbote im Bereich des Verfassungsschutzes entsprechen der Regelung in § 23 Nr. 2 BVerfSchG und sind damit ebenso wenig zur Auflösung des Zielkonfliktes geeignet. Ein hinreichendes Gesamtsystem, das zur effektiven Sicherung von informationstechnischen Schwachstellen führt und auf das sich der Bundesgesetzgeber zur Rechtfertigung seiner Untätigkeit berufen könnte, liegt damit nicht vor. Vielmehr existiert lediglich ein Flickenteppich an unzureichenden Landesregelungen.

(7) Untergesetzliche Regelungen unzureichend

Untergesetzliche Regelungen sind bereits generell unzureichend.

Vorliegend geht es um Maßnahmen von hoher Eingriffsintensität, welche Schutzvorkehrungen im Sinne eines Schwachstellenmanagements erforderlich machen. Um dem Wesentlichkeitsprinzip gerecht zu werden, bedarf es bei Eingriffen mit hoher Grundrechtsrelevanz eines bestimmten und normenklaren Parlamentsgesetzes, was untergesetzliche Verwaltungsvorschriften oder auch vertragliche Regelungen zur Erfüllung des Schwachstellenmanagements ausschließt (hierzu bereits **a)**).

Ein Großteil der untergesetzlichen Regelungen entzieht sich zudem dem Kenntnisstand der Beschwerdeführer*innen. So stellt auch die Cybersicherheitsstrategie 2021 dar:

> Die Nutzung von Zero-Day-Schwachstellen zu Zwecken der nachrichtendienstlichen Aufklärung, Gefahrenabwehr und Strafverfolgung erfolgt aktuell nach den für die jeweilige Sicherheitsbehörde geltenden internen Behördenvorgaben.
>
> BMI-Cybersicherheitsstrategie für Deutschland – August 2021 (Punkt 8.3.10), abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=83662AC1E20FC5105001A4124D56545C.2_cid364?__blob=publicationFile&v=1.

Außenstehende haben keinen Zugriff auf derartige internen Behördenvorgaben. So sind beispielsweise Dienstanweisungen unter Verschluss, mindestens mit dem VS-Grad „NfD – Nur für den Dienstgebrauch“, vorliegend eher mit dem VS-Grad „geheim“ oder „streng geheim“ und damit dem Zugang der Beschwerdeführer*innen verwehrt. Selbst wenn die Beschwerdeführer*innen aber vollumfänglich Zugang zu den entsprechenden Vorgaben hätten, könnte das entsprechende Regelungsgeflecht nicht hinreichend dargestellt werden, da untergesetzliche Regelungen jederzeit geändert werden können.

Die öffentlich zugänglichen untergesetzlichen Regelungen sind auch über diese formellen Mängel hinaus inhaltlich nicht ausreichend, um das verfassungsrechtlich gebotene Schwachstellenmanagement abbilden zu können. Diese nehmen die nachrichtendienstliche Übermittlung zu Sicherheitslücken von den Meldeverpflichtungen ebenso aus, wie die einfachgesetzliche Ebene. Dies gilt zunächst für die innerhalb der Bundesverwaltung geltende Allgemeine Verwaltungsvorschrift über das Meldeverfahren im Sinne von § 4 Abs. 6 BSIG (hierzu bereits **(3)**). Gleiches betrifft die mit Beschluss 2017/35 des IT-Planungsrates getroffene Übereinkunft zu gemeinsamen Meldestandards in-

nerhalb des VCV, die den Informationsaustausch zwischen Bund und Ländern regelt.

Normenhierarchisch gehen die jeweiligen Übermittlungsverbote in den Bundesländern für die Landesämter für Verfassungsschutz, die im Rahmen ihrer Befugnisse ebenfalls gem. §§ 9, 11 Abs. 1 G 10 mit der Pflicht zum Schwachstellenmanagement in Berührung kommen, den beschlossenen Meldestandards vor.

> Vgl. § 11 Abs. 1 Nr. 2 LVSG, Art. 27 Abs. 1 Nr. 2 BayVSG, § 28 Nr. 2 VSG Bln, § 19 Abs. 1 Nr. 3 BbgVerfSchG, § 23 Abs. 1 Nr. 4 BremVerfSchG, § 21 Abs. 1 Nr. 2 HmBVerfSchG, § 23 Abs. 1 Nr. 2 HVSG, § 25 Abs. 1 Nr. 2 LVerfSchG M-V, § 19 Nr. 2 VSG NRW, § 27 Nr. 2 LVerfSchG RhPf, § 13 Abs. 1 S.1 Nr. 2 SächsVSG, § 20 Nr. 2 VerfSchG-LSA, § 19 Abs. 1 Nr.2 SVerfSchG, § 24 Abs. 1 Nr. 2 LVerfSchG SH, § 22 Abs. 1 Nr. 2 ThürVerfSchG.

Zudem lässt die öffentlich zugängliche Responsible Disclosure Policy (RDP) des Länder-CERT-NRW darauf schließen, dass Verschlusssachen von der Übermittlung im VCV ausgenommen sind.

> Vgl. CERT NRW, Responsible Disclosure Policy, S. 3, abrufbar unter https://www.it.nrw/sites/default/files/atoms/files/cert_nrw-responsible-disclosure-policy_de.pdf.

Sicherheitslücken, die zum Zwecke des Einsatzes der Quellen-Telekommunikationsüberwachung ausgenutzt werden sollen, werden also im Regelfall bereits nicht vom Meldeverfahren im VCV erfasst.

Ein untergesetzliches Schwachstellenmanagement wird somit den Landesbehörden überlassen, bleibt jedoch nach dem Beschluss des IT-Planungsrates 2022/08 in vielen Bundesländern, die noch keine CERT-Struktur aufweisen, mehr unverbindliches Ziel denn Pflicht.

> Vgl. IT-Planungsrat, CERT-Standard, abrufbar unter https://www.it-

planungsrat.de/fileadmin/beschluesse/2022/Beschluss2022-08_Mindeststandard_CERT.pdf.

Selbst wenn dieses Ziel erreicht werden sollte, können untergesetzliche landesrechtlich unterschiedlich ausgestaltete Regelungen zum Schwachstellenmanagement nicht die staatliche Schutzpflicht erfüllen. Vielmehr bedarf es eines hinreichend bestimmten Parlamentsgesetzes, welches den entstandenen Zielkonflikt einheitlich für das gesamte Bundesgebiet adressiert (hierzu bereits **a)**).

(8) Gesamtsystem nicht hinreichend

In der Gesamtschau ergibt sich auch aus dem Zusammenspiel der vorgetragenen Regelungen kein hinreichendes Schwachstellenmanagement.

Im Zentrum des bundesrechtlich intendierten Schwachstellenmanagements steht das BSI, das Meldungen von Behörden der Länder und des Bundes sowie Dritten entgegennimmt, auswertet und gegebenenfalls eine Offenlegung der Schwachstelle beschließt. Das BSI kann dieser vorgesehenen Rolle allerdings nur bedingt nachkommen, da es sich bei konkreter Betrachtung nur in ein beschränktes Meldesystem eingebettet sieht, das eine bedeutende Anzahl an Wissensträger*innen um Sicherheitslücken von der Unterrichtungspflicht ausnimmt. Das BSI verliert damit gerade in Bezug auf das Management von Zero-Day-Schwachstellen seine Bedeutung zugunsten der Nachrichtendienste. Dies birgt erhebliches Gefahrenpotenzial für Millionen von Nutzer*innen, da keine transparenten, hinreichend bestimmten gesetzlichen Kriterien vorgegeben werden.

Somit stehen sich der staatlichen Schutzpflicht dienenden Stellen wie das BSI und die Nachrichtendienste gegenüber, die von dem Offenhalten von Sicherheitslücken profitieren. Gleichzeitig hält der Gesetzgeber kein System vor, nach welchem sich dieser Zielkonflikt verfassungskonform auflösen lassen könnte.

Die Mängel in diesem System werden auch nicht durch ergänzende Regelungen bspw. des Datenschutzrechts oder europarechtliche Vorgaben kompensiert. Dies gestehen auch die Regierungsparteien ein, die sich die Einführung eines wirksamen Schwachstellenmanagements in ihrem Koalitionsvertrag vorgenommen haben.

> Vgl. Mehr Fortschritt Wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), S. 13.

Die Bundesregierung plant zwar höhere Eingriffsschwellen für Maßnahmen des Verfassungsschutzes und hat ein Gutachten der Wissenschaftlichen Dienste in Auftrag gegeben und laut Medienberichten eine Arbeitsgruppe eingerichtet.

> Vgl. Wie die Bundesregierung den Verfassungsschutz einhegen will, Süddeutsche Zeitung vom 20. Juni 2022, abrufbar unter https://www.sueddeutsche.de/politik/verfassungsschutz-reform-bundesregierung-karlsruhe-1.5605167?reduced=true; sowie das Gutachten: Ausarbeitung des Wissenschaftlichen Dienstes, Auswirkungen des Urteils des Bundesverfassungsgerichts vom 26. April 2022 zum Bayerischen Verfassungsschutzgesetz, WD 3 - 3000 - 068/22.

Allerdings geht es darin um die Übertragbarkeit des Urteils des angerufenen Gerichts zum *Bayrischen Verfassungsschutzgesetz* auf entsprechende Vorschriften im Bundesverfassungsschutzgesetz, BND-Gesetz und MAD-Gesetz und um die Auswirkungen auf das BKA-Gesetz. Die vorliegend gerügten Vorschriften sind hingegen nicht Teil des Gutachtens, das Artikel 10-Gesetz wird nicht auf Mängel untersucht. Somit beziehen sich auch nicht etwaige Reformvorschläge auf die vorliegend angegriffenen Regelungen, vielmehr bestehen noch keine konkreten Schritte zur gesetzlichen Regelung eines Schwachstellenmanagements.

IV. Übermittlungsvorschriften (§ 4 Abs. 4 G 10)

Auch die Übermittlungsvorschrift des § 4 Abs. 4 G 10 verstößt gegen die verfassungsrechtlichen Anforderungen. Dies gilt sowohl für § 4 Abs. 4 Satz 1 G 10, der die Übermittlung an innerstaatliche Stellen regelt, als auch für § 4 Abs. 4 Satz 2 G 10, der die Übermittlung an ausländische öffentliche Stellen betrifft.

1. Maßstab

Nach der Rechtsprechung des angerufenen Gerichts stellt die Übermittlung von Daten eine zweckändernde Nutzung dieser Daten dar, da die ursprüngliche Nutzung stets nur die Verwendung durch die erhebende Behörde umfasst.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 230.

Damit besteht ein eigenständiger Grundrechtseingriff. Dieser ist an dem Grundrecht zu messen, in das bei der ursprünglichen Datenerhebung eingegriffen wurde.

> Vgl. BVerfGE 154, 152 <266 Rn. 212>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 230.

Dies sind bei den Maßnahmen der § 11 Abs. 1a Satz 1 und 2 G 10 das Fernmeldegeheimnis (hierzu **I.1**) und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (hierzu **II.1**).

Maßgebend für die Verhältnismäßigkeit derartiger Maßnahmen ist das Kriterium der hypothetischen Datenneuerhebung. Danach kommt es darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben werden dürften. Daraus ergeben sich Anforderungen, die sowohl an den Rechtsgüterschutz als auch an die Übermittlungsschwellen zu stellen sind.

BVerfGE 141, 220 <327 f. Rn. 287>; 154, 152 <266 f. Rn. 216>; 156, 11 <49 f. Rn. 99>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 231 stRspr.

Die konkreten Übermittlungsanforderungen können sich dabei danach unterscheiden, je nachdem, an welche Behörde übermittelt wird. Dabei ist insbesondere von Relevanz, ob die empfangende Behörde über operative Anschlussbefugnisse verfügt. In diesem Fall sind aufgrund der unmittelbar möglichen Folgemaßnahmen strengere Anforderungen zu stellen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 234.

Werden Daten an ausländische Behörden weitergegeben, setzt die Übermittlung zudem einen datenschutzrechtlich angemessenen und mit elementaren Menschenrechtegewährleistungen vereinbaren Umgang mit den übermittelten Daten im Empfängerstaat sowie eine entsprechende Vergewisserung hierüber seitens des deutschen Staates voraus.

BVerfGE 141, 220 <344 Rn. 332>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 260.

Diese Voraussetzungen erfüllen § 4 Abs. 4 Satz 1 und 2 G 10 nicht.

2. Übermittlung an inländische Stellen, § 4 Abs. 4 Satz 1 G 10

Weder die in § 4 Abs. 4 Satz 1 Nr. 1 G 10 normierten Übermittlungsbefugnisse an Gefahrenabwehrbehörden mit operativen Anschlussbefugnissen (hierzu **a)**), noch die Befugnisse zur Übermittlung an Strafverfolgungsbehörden in § 4 Abs. 4 Satz 1 Nr. 2 G 10, (hierzu **b)**) werden dem verfassungsrechtlichen Maßstab gerecht. Auch § 4 Abs. 4 Satz 1 Nr. 3 G 10 ist unzureichend, da die Befugnis zur Übermittlung an sonstige Stellen keine besonderen Anforderungen für die Übermittlung an mit operativen Anschlussbefugnissen ausgestatteten Behörden aufstellt (hierzu **c)**).

a) Übermittlung an Gefahrenabwehrbehörden, § 4 Abs. 4 Satz 1 Nr. 1 G 10

Das angerufene Gericht fordert für die Übermittlung von personenbezogenen Daten durch die Nachrichtendiensten an Gefahrenabwehrbehörden mit operativen Anschlussbefugnissen, dass wenigstens eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut besteht, mithin ein herausragendes öffentliches Interesse an der Übermittlung besteht.

> BVerfGE 133, 277 <329 Rn. 123>; 154, 152 <268 Rn. 219>; 156, 11 <51 f. Rn. 105, 55 Rn. 116>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 235.

Diesen Anforderungen wird die Vorschrift nicht gerecht. Weder verlangt die Vorschrift das Vorliegen einer konkretisierten Gefahr (hierzu **(1)**), noch schützen sämtliche der in Bezug genommenen Delikte besonders gewichtige Rechtsgüter (hierzu **(2)**). Zuletzt weist die Regelungsstruktur Mängel auf, da sie dem Grundsatz der Normenklarheit nicht gerecht wird (hierzu **(3)**). Die Defizite werden auch nicht durch enthaltene Verfahrensvorschriften kompensiert (hierzu **(4)**).

(1) Fehlendes Erfordernis der konkretisierten Gefahr

So fehlt es bereits an der Voraussetzung einer konkretisierten Gefahr.

Gemäß § 4 Abs. 4 Satz 1 Nr. 1 lit. a) G 10 ist eine Übermittlung bereits möglich, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine Straftat plant oder begeht. Damit unterschreitet das Gesetz die verfassungsrechtlichen Anforderungen in mehrfacher Hinsicht.

So ist bereits der Begriff der tatsächlichen Anhaltspunkte nicht ausreichend. Dieser wird zudem dadurch relativiert, dass lediglich ein Verdacht dafür bestehen muss, dass jemand eine Straftat plant.

Zwar fordert § 4 Abs. 4 Satz 1 Nr. 1 lit. b) G 10 bestimmte Tatsachen. Auch hier wird der Maßstab jedoch dadurch heruntergesetzt, dass diese Tatsachen lediglich den Verdacht begründen müssen, dass eine Person eine Straftat plant.

Diese zu geringe Eingriffsschwelle wird auch nicht durch die Maßgabe abgemildert, dass Daten lediglich übermittelt werden dürfen, wenn dies für die Aufgabenerfüllung der empfangenden Behörde erforderlich ist. Die Erforderlichkeit auf Seiten der empfangenden Zielbehörde betrifft die Frage, wann diese überhaupt Daten anfordern oder auswerten kann. Dies ist aber strikt zu trennen von der Frage, ab welcher Schwelle die Ausgangsbehörde eine Übermittlung durchführen darf.

Vgl. BVerfGE 155, 119 <209 f. Rn. 201>.

Zudem wird die übermittelnde Behörde regelmäßig nicht einschätzen können, wann eine Übermittlung aus Empfängersicht erforderlich sein wird. Die Zielbehörde hingegen wird regelmäßig das Empfangen weiterer Daten für ihre eigene Aufgabenerfüllung für erforderlich erachten. Mehr Daten bedeuten immer mehr Informationen zur Erkenntnisgewinnung. Für die Ermittlung der Erforderlichkeit als maßgebliches Kriterium für eine Datenübermittlung sind mithin keinerlei Vorgaben getroffen. Folglich ist davon auszugehen, dass eine Übermittlung praktisch in nahezu jedem Fall seitens der Behörden als erforderlich angesehen wird. Damit wird das Kriterium der Erforderlichkeit ausgehöhlt und stellt keine ernsthafte Einschränkung des Übermittlungstatbestandes dar.

(2) Fehlendes Erfordernis des Schutzes herausragender Rechtsgüter

Auch die Anforderungen an die zu schützenden Rechtsgüter sind nicht erfüllt.

Nach der Rechtsprechung des angerufenen Gerichts ist eine Übermittlung zum Schutz von Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes möglich. Daneben darf eine Übermittlung auch zugunsten des Schutzes von Sachen von bedeutendem Wert, beispielsweise

wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen stattfinden.

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 243, 251.

Das ist bei den in Bezug genommenen Strafnormen nicht durchgängig der Fall.

So verweist § 4 Abs. 4 Satz 1 Nr. 1 lit. a) G 10 auf den Straftatenkatalog der § 3 Abs. 1 Satz 1 und 1a G 10. Dieser verweist wiederum auf Straftaten, die teils als Delikte im Bereich der Bagatelle oder mittleren Kriminalität einzuordnen sind (hierzu bereits **I.3.a)(2)(c)**). Daneben setzen sich die bereits aufgezeigten Mängel auch im Rahmen des § 4 Abs. 4 Satz 1 Nr. 1 lit. b) i.V.m. § 7 Abs. 4 G 10 in ähnlicher Form fort.

Erstens unterschreiten die in § 7 Abs. 4 Satz 1 Nr. 1 lit. a), c) G 10 genannten Delikte teilweise die für eine Übermittlung vorauszusetzenden Schutzgüter in Teilen, indem diese vorrangig den Schutz der Allgemeininteressen an der Sicherheit und Zuverlässigkeit des Zahlungs- und Wertpapierverkehrs, der Funktionsfähigkeit der Rechtspflege sowie am Schutz vor Drogenkriminalität bezwecken:

> §§ 146, 151, 152, 152a, 261 StGB, § 29a Abs. 1 Nr. 2, 30 Abs. 1 Nr. 1, 4, 30a BtMG.

Zweitens gilt dies erst recht in Anbetracht der gemäß § 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 StPO in Bezug genommenen weiteren Delikte. Viele der in § 100a Abs. 2 StPO normierten Delikte lassen zwar ein gesteigertes öffentliches Interesse an der Strafverfolgung erkennen. Gleichzeitig weichen diese ebenfalls vom Schutz herausragender Rechtsgüter ab. Hierzu zählen beispielsweise die nachgehend aufgeführten Normen im Strafgesetzbuch, welche vorrangig die öffentliche Sicherheit und Ordnung, das Eigentum, das Individualvermögen, den Wettbewerb, die Funktionsfähigkeit des öffentlichen Dienstes und die Insolvenzmasse vor Verringerung schützen. Überdies dienen einige der Delikte dem Schutz des Allgemeininteresses an einer effektiven staatlichen Wirtschaftsförderung, an der Sicherstellung des Aufkommens der

Mittel für die Sozialversicherung und an der Zuverlässigkeit des Rechtsverkehrs, insbes. des Beweisverkehrs mit Urkunden:

> § 100a Abs. 2 Nr. 1 lit. d) StPO i.V.m. § 127 Abs. 3 StGB i.V.m. § 127 Abs. 1 Nr. 2 a) (z.B. mit Bezugstaten der §§ 202 a ff. StGB oder §§ 259 ff. StGB),
>
> § 100a Abs. 2 Nr. 1 lit. j) StPO i.V.m. § 244 Abs. 1 Nr. 2 StGB, § 244 Abs. 4 StGB oder § 244a StGB,
>
> § 100a Abs. 2 Nr. 1 lit. l) StPO i.V.m. § 260 StGB oder § 260a StGB,
>
> § 100a Abs. 2 Nr. 1 lit. n) StPO i.V.m. § 263 Abs. 3 Satz 2 StGB oder § 263 Abs. 5 StGB, jeweils auch i.V.m. § 263a Abs. 2 StGB,
>
> § 100a Abs. 2 Nr. 1 lit. o) StPO i.V.m. § 264 Abs. 2 Satz 2 oder § 264 Abs. 3 i.V.m. § 263 Abs. 5,
>
> § 100a Abs. 2 Nr. 1 lit. p) StPO i.V.m. § 265e Satz 2 StGB,
>
> § 100a Abs. 2 Nr. 1 lit. q) StPO i.V.m. § 266a Abs. 4 Satz 2 Nr. 4 StGB,
>
> § 100a Abs. 2 Nr. 1 lit. r) StPO i.V.m. § 267 Abs. 3 Satz 2 StGB, § 267 Abs. 4 StGB jeweils auch i.V.m. § 268 Abs. 5 StGB, § 269 Abs. 3 StGB oder nach § 275 Abs. 2 StGB und § 276 Abs. 2 StGB,
>
> § 100a Abs. 2 Nr. 1 lit. s) StPO i.V.m. § 283a Satz 2 StGB,
>
> § 100a Abs. 2 Nr. 1 lit. t) StPO i.V.m. § 298 StGB oder i.V.m. §§ 300 Satz 2, 299 StGB,
>
> § 100a Abs. 2 Nr. 1 lit. u) StPO i.V.m. § 306 StGB, § 332 StGB oder § 334 StGB.

Drittens und letztens verweist § 4 Abs. 4 Satz 1 Nr. 1 lit. b) G 10 auf § 7 Abs. 4 Satz 1 G 10, der ebenfalls zahlreiche Straftaten enthält, die kein ausreichend erhebliches Rechtsgut schützen. So enthält § 89b Abs. 1 StGB nur einen Strafrahmen von bis zu drei Jahren Freiheitsstrafe und § 146 Abs. 1 StGB sogar von nur einem Jahr.

(3) Verfehlung des Gebots der Normenklarheit

Schlussendlich verfehlt die Übermittlungsvorschrift den durch das angerufene Gericht aufgestellten Grundsatz zur Normenklarheit.

Danach kommt eine Verletzung des Gebots der Normenklarheit in Betracht, wenn der Gesetzgeber vielgliedrige Verweisungsketten verwendet. An einer normenklaren Rechtsgrundlage fehlt es zwar nicht schon deshalb, weil in einer Norm auf eine andere Norm verwiesen wird. Doch müssen Verweisungen begrenzt bleiben, dürfen nicht durch die Inbezugnahme von Vorschriften, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis nicht zu übermäßigen Schwierigkeiten bei der Anwendung führen. Unübersichtliche Verweisungskaskaden, die jedenfalls sechs unterschiedliche Verweisungen beinhalten, sind mit den grundrechtlichen Anforderungen insofern nicht vereinbar. Dabei sind auch Verweisungen innerhalb derselben Norm zu berücksichtigen.

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 272, 391.

Das verfassungsrechtliche Maß ist überschritten, da der Gesetzgeber mit § 4 Abs. 4 Satz 1 Nr. 1 lit. b) G 10 i.V.m. § 7 Abs. 4 Satz 1 Nr. 2 G 10 beispielsweise unter Inbezugnahme des § 100a Abs. 2 StPO, zahlreiche mindestens sechsgliedrige Verweisungsketten vorsieht. In Anbetracht der großen Anzahl der über § 100a Abs. 2 StPO in Betracht kommenden Verweisungsketten wird sich der Übersichtlichkeit halber stellvertretend auf die nachgenannten Beispiele beschränkt.

Die Übermittlung zu Strafverfolgungszwecken wegen der geplanten Begehung eines Betruges als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Urkundsdelikten zusammengeschlossen hat, würde sich dann beispielsweise nachfolgender Verweisungskette richten:

> § 4 Abs. 4 Satz 1 Nr. 1 lit. b) G 10 i.V.m. § 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. n) StPO i.V.m. § 263a Abs. 1 StGB i.V.m. § 263a Abs. 2 StGB i.V.m. § 263 Abs. 5 StGB i.V.m. § 267 StGB.

Ähnlich verhielte es sich bei der Übermittlung zu Strafverfolgungszwecken wegen Anhaltspunkten zu einer geplanten Geldwäsche, die einen schweren Bandendiebstahl mit Waffen zur Vortat hatte. Die entsprechende Verweisungskette ist ebenfalls nicht mehr normenklar:

> § 4 Abs. 4 Satz 1 Nr. 1 lit. b) G 10 i.V.m. § 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. n) stopp i.V.m. § 100a Abs. 2 Nr. 1 lit j) StPO i.V.m. § 261 StGB i.V.m. § 244a Abs. 1 StGB i.V.m. § 244 Abs. 1 Nr. 1 lit. a) StGB. Im Hinblick auf § 261 Abs. 4 StGB könnte diese Verweisungskette sogar noch anwachsen.

Die Verweisungsketten lassen sich je nach konkreter Tatbestandsvariante des § 263 Abs. 5 StGB i.V.m. §§ 263, 264, 268, 269 StGB oder des § 244a StGB i.V.m. §§ 243 Abs. 1, 244 Abs. 1 Nr. 3 StGB oder § 244 Abs. 4 StGB beliebig modifizieren und umfassen somit eine große Anzahl an denkbaren Delikten.

Schließlich lässt sich die Unübersichtlichkeit der Verweisungen anhand von § 4 Abs. 4 Satz 1 Nr. 1 lit. a) G 10 exemplarisch betrachten, der i.V.m. § 3 Abs. 1a G 10 i.V.m. § 3 Abs. 1 Satz 1 Nr. 1 G 10 i.V.m. § 72 Abs. 1, 3 ZFdG i.V.m. den dort genannten Delikten der § 19 Abs. 1 oder Abs. 2, § 20 Abs. 1, § 20a Abs. 1 oder Abs. 2 oder § 22a Abs. 1 Nr. 4, 5 oder 7 oder Abs. 2 des Gesetzes über die Kontrolle von Kriegswaffen (KrWaffKontrG) unter Beeinträchtigung der Normenklarheit ebenfalls eine Vielzahl an Normgliedern beinhaltet.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 391.

(4) Keine Kompensation durch Verfahrensvorschriften

Die Absicherungen in § 4 Abs. 5 und 6 G 10 kompensieren den unverhältnismäßigen Eingriff nicht. Die dort enthaltenen Verfahrenssicherungen vermögen ebenfalls nicht darüber hinwegzuhelfen, dass die gewählten Eingriffsschwellen und die zu schützenden Rechtsgüter nicht den verfassungsrechtlichen Vorgaben entsprechen. Denn bei der Anwendung dieser Verfahrenssicherungen wird der Maßstab der vorhandenen, zu geringen Eingriffsschwellen zugrunde gelegt.

b) Übermittlung an Strafverfolgungsbehörden, § 4 Abs. 4 Satz 1 Nr. 2 G 10

Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es für die Zulässigkeit der Übermittlung auf das Gewicht der Straftaten an. Orientierungspunkt ist dabei die gesetzgeberische Einteilung in erhebliche, schwere und besonders schwere Straftaten. Nach der Rechtsprechung des angerufenen Gericht ist eine Übermittlung nur zum Schutz eines herausragenden öffentlichen Interesses und daher nur zur Verfolgung besonders schwerer Straftaten möglich.

> BVerfGE 154, 152 <269 Rn. 221>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 251.

Diesen Anforderungen entsprechen die hier in Bezug genommenen Straftaten nicht der Fall. Der Gesetzgeber hat selbst besonders schwere Straftaten in § 100b Abs. 2 StPO näher bestimmt. Die Anlasstaten des § 4 Abs. 4 Satz 1 Nr. 2 G 10 gehen weit darüber hinaus und umfassen unter anderem auch Bagatelldelikte (hierzu bereits **I.3.a)(2)(c)**).

Konkret überschreiten die über die folgenden Verweisungen in Bezug genommenen Delikte den durch § 100b Abs. 2 StPO konkretisierten Rahmen:

- § 4 Abs. 4 Nr. 2 i.V.m. Nr. 1 lit. b) i.V.m. § 7 Abs. 4 Nr. 2 G 10 i.V.m. § 100a Abs. 2 StPO:
    - §§ 80a, 84, 85, 86, 87, 88, 89, 95 Abs. 1 bis 2, 96 Abs. 2, 97, 97b, 98 Abs. 1 Satz 1, Abs. 2, 99 Abs. 1, 3, 100a Abs. 1 bis 3, 108e, 109d bis 109h StGB,
    - § 127 Abs. 3 und 4 StGB wobei die Zweckbindung sich auf die Förderung oder Ermöglichung besonders schwerer Straftaten nach § 100a Abs. 2 StPO (und nicht § 100b Abs. 2 StPO) bezieht,

- §§ 129 Abs. 1 bis 4 ohne Regelbeispiel nach Abs. 5 StGB, 129a Abs. 3, auch in Verbindung mit Abs. 5 Satz 1 Alt. 2 oder Satz 2, 130 StGB,
- § 176 Abs. 2 StGB,
- § 264 Abs. 2 Satz 2, Abs. 3 in Verbindung mit § 263 Abs. 5, 265e Satz 2, 266a Absatz 4 Satz 2 Nummer 4, 267 Abs. 3 Satz 2, 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, § 275 Abs. 2 und § 276 Abs. 2, § 283a Satz 2, § 298, § 299 i.V.m. § 300, 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316 StGB,
- § 17 Abs. 4, 5, § 18 Abs. 1 bis 6, 9, 11 bis 12 AWG,
- §§ 19 Abs. 1, 3, 20a Abs. 1 bis 3, § 22a Abs. 1 bis 3 KrWaff-KontrG,
- § 19 Abs. 1 GÜG,
- § 51 Abs. 1 bis 3, § 52 Abs. 1 Nr. 3 lit. c) und d), Abs. 6 WaffG,
- Steuerstraftaten nach § 100a Abs. 2 Nr. 2 StPO i.V.m. AO
    - Steuerhinterziehung unter den in § 370 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzungen, sofern der Täter als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Taten nach § 370 Absatz 1 verbunden hat, handelt, oder unter den in § 370 Absatz 3 Satz 2 Nummer 5 genannten Voraussetzungen,
    - gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,
    - Steuerhehlerei im Falle des § 374 Abs. 2,
- Straftaten unter Verstoß gegen § 4 Abs. 4 Nr. 2 lit. b) Anti-Doping-Gesetz und

- Straftaten nach § 13 Absatz 3 Ausgangsstoffgesetz

- § 4 Abs. 4 Nr. 2 i.V.m. Nr. 1 lit. a) i.V.m. § 3 Abs. 1, Abs. 1a G 10:
  - § 83 StGB
  - § 89b StGB, § 20 Abs, 1 Nr. 1 bis 4 VereinsG,
  - §§ 202a, 202b und 303a, 303b StGB, soweit sich die Straftat gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet,
  - §§ 316b Abs. 3, 316c Abs. 1 und 3 StGB und
  - § 95 Abs. 1 Nr. 8 AufenthG.

Zudem teilt auch § 4 Abs. 4 Satz 1 Nr. 2 G 10 die Mängel von Nr. 1 in Bezug auf die Normenklarheit, da diese an die dort in Bezug genommenen Straftaten anknüpft.

c) Übermittlung an sonstige Stellen, § 4 Abs. 4 Satz 1 Nr. 3 G 10

Auch die Übermittlung an sonstige Stellen in § 4 Abs. 4 Satz 1 Nr. 3 G 10 entspricht nicht den verfassungsrechtlichen Anforderungen. Nur zum Schutz eines Rechtsguts von besonderem Gewicht dürfen Daten an solche Stellen übermittelt werden.

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 255.

Besonders strenge Vorgaben gelten auch hier, wenn die empfangende Stelle über operative Anschlussbefugnisse verfügt.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 255, 258.

§ 4 Abs. 1 Satz 1 Nr. 3 G 10 geht über diese Vorgaben hinaus. Die Vorschrift ermöglicht die Übermittlung bereits zur Vorbereitung und Durchführung eines Verfahrens nach Art. 21 Abs. 2 Satz 2 GG oder einer Maßnahme nach § 3 Abs. 1 Satz 1 des Vereinsgesetzes (VereinsG).

Bereits der Verweis auf Art. 21 Abs. 2 Satz 2 GG geht fehl. Dort war bis zum 20. Juli 2017 das Parteiverbotsverfahren geregelt. Die entsprechende Regelung findet sich nunmehr in Art. 21 Abs. 4 GG. Indem der Gesetzgeber aktuelle Änderungen im Artikel 10-Gesetz vorgenommen hat, allerdings diesen veralteten Verweis nicht aktualisierte, liegt ein Verstoß gegen das Gebot der Normenklarheit vor.

§ 3 Abs. 1 VereinsG regelt das Vereinsverbot. Zuständige Behörde ist entweder die oberste Landesbehörde oder die nach Landesrecht zuständige Behörde (§ 3 Abs. 2 Satz 1 Nr. 1 VereinsG) oder aber das Bundesministerium des Innern und für Heimat (§ 3 Abs. 2 Satz 1 Nr. 2 VereinsG). Indem die Ermächtigung im Bereich der Länder nicht auf die oberste Landesbehörde beschränkt wird, ist nicht ausgeschlossen, dass auch Behörden mit operativen Anschlussbefugnissen erfasst werden. Die Übermittlung an diese unterliegt aber strengeren Voraussetzungen, als § 4 Abs. 4 Satz 1 Nr. 3 G 10 vorsieht.

Die beiden Verbotsverfahren dienen zwar dem Erhalt der verfassungsmäßigen Ordnung. Allerdings dürfen die Daten bereits zur „Vorbereitung“ übermittelt werden. Dies bedeutet, dass eine Datenübermittlung bereits zu einem Zeitpunkt stattfindet, an dem noch gar nicht feststeht, ob eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut – Leib, Leben und Freiheit der Person, Bestand oder Sicherheit des Bundes oder eines Landes sowie Sachen von bedeutendem Wert – wirklich gegeben ist.

Darüber hinaus ist unklar, was überhaupt unter der „Vorbereitung“ der entsprechenden Maßnahmen zu verstehen ist. Lediglich Erkenntnisse, welche die Verfassungswidrigkeit eines Vereins belegen, sind zur „Durchführung“ einer Maßnahme nach § 3 Abs. 1 VereinsG notwendig. Dementsprechend gehen Daten zur Vorbereitung deutlich darüber hinaus. Wie weit derartige Informationen aber reichen dürfen, ergibt sich nicht aus der Vorschrift. Da regelmäßig sämtliche verfügbaren Informationen zur Vorbereitung einer derartigen Maßnahme zumindest hilfreich sein können, auch wenn diese noch lange keine verfassungswidrigen Bestrebungen belegen, fehlt es an einer hinreichenden

normativen Begrenzung. Mithin bestehen auch erhebliche Zweifel hinsichtlich der Bestimmtheit und Normenklarheit der Vorschrift.

3. Übermittlung an ausländische Stellen, § 4 Abs. 4 Satz 2 G 10

Auch die Übermittlung an ausländische Stellen nach § 4 Abs. 4 Satz 2 G 10 entspricht nicht den verfassungsrechtlichen Vorgaben.

Hierbei richten sich die Anforderungen ebenfalls nach dem Kriterium der hypothetischen Datenneuerhebung. Darüber hinaus setzt die Übermittlung einen datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen zu vereinbarenden Umgang mit den übermittelten Daten im Empfängerstaat und eine entsprechende Vergewisserung hierüber seitens des deutschen Staats voraus.

> BVerfGE 154, 152 <273 Rn. 232>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 260.

§ 4 Abs. 4 Satz 2 G 10 knüpft zunächst an die Voraussetzungen des § 4 Abs. 4 Satz 1 G 10 an und teilt damit bereits dessen verfassungsrechtliche Mängel.

Darüber hinaus sind aber auch die weiteren Anforderungen, die spezifisch für Übermittlungen ins Ausland gelten, nicht erfüllt.

§ 4 Abs. 4 Satz 2 G 10 verweist auf § 19 Abs. 3 Satz 2 und 4 BVerfSchG. Danach unterbleibt die Übermittlung, wenn auswärtige Belange der Bundesrepublik oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen (§ 19 Abs. 3 Satz 2 BVerfSchG). Zudem muss die empfangene Stelle darauf hingewiesen werden, dass die übermittelten Daten nur zum Zweck verwendet werden dürfen, zu dem diese übermittelt wurde und sich die sendende Behörde vorbehält, Auskunft über die vorgenommene Verwendung der Daten zu erbitten (§ 19 Abs. 3 Satz 4 BVerfSchG).

Damit besteht gerade keine Einschränkung dahingehend, dass elementare Menschenrechtsgewährleistungen einzuhalten sind und die übermittelnde Behörde sich dessen auch vergewissern muss.

Auch „überwiegend schutzwürdige Interessen des Betroffenen“ (§ 19 Abs. 3 Satz 2 BVerfSchG) setzen diese Anforderung nicht in hinreichend bestimmter und normenklarer Art um. Selbst wenn dies aber der Fall wäre, würde sich daraus keine bestimmte und normenklare Vergewisserungspflicht der übermittelnden Behörde ergeben.

V. Informationssystem der Nachrichtendienste (§ 6 Abs. 1, Abs. 2 BVerfSchG, § 3 Abs. 3 MADG)

Das in § 6 Abs. 1 und 2 BVerfSchG und § 3 Abs. 3 MADG verankerte Informationssystem der Nachrichtendienste verletzt das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG der Beschwerdeführer*innen. In diesem System besteht eine Übermittlungspflicht zwischen den einzelnen Verfassungsschutzbehörden bezüglich aller relevanten Information, § 6 Abs. 1 Satz 1 BVerfSchG. Dieser Übermittlungspflicht kommen die Dienste durch die Teilnahme am gemeinsamen nachrichtendienstlichen Informationssystem nach, § 6 Abs. 2 Satz 1 BVerfSchG. Auch für den MAD besteht eine derartige Übermittlungspflicht, § 3 Abs. 3 Satz 1 MADG. Für diesen besteht die Option, hierzu am nachrichtendienstlichen Informationssystem teilzunehmen, § 3 Abs. 3 Satz 2 MADG, § 6 Abs. 2 Satz 2 BVerfSchG.

Bei der Durchführung des Informationssystems handelt es sich sowohl bei der Speicherung im System als auch beim Abruf der Daten um Eingriffe in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (hierzu **1.**). Derartige Eingriffe durch ein vergleichbares System sind in der Rechtsprechung des angerufenen Gerichts noch nicht abschließend geklärt. Dennoch lassen sich der Rechtsprechung zu verwandten Rechtsfragen sowie zur Datenübermittlung allgemein verfassungsrechtliche Grundsätze entnehmen, die auch in Bezug auf das vorliegende Informationssystem zur Anwendung kommen müssen (hierzu **2.**). Die konkreten Regelungen gehen in ihrer Intensität und Ausgestaltung weit über den verfassungsrechtlichen Rahmen hinaus (hierzu **3.**).

1. Grundrechtseingriffe

Nach der Rechtsprechung des angerufenen Gerichts greifen sowohl die Speicherung als auch die Analyse von in einer Verbunddatei gespeicherten Daten unabhängig voneinander in das Recht auf informationelle Selbstbestimmung

aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein. Soweit die von der Speicherung betroffenen Daten durch Eingriffe in Art. 10 Abs. 1 GG oder Art. 13 Abs. 1 GG erhoben wurden, ist die Folgeverwendung auch an diesen Grundrechten zu messen.

BVerfGE 133, 277 <317 Rn. 95>.

2. Maßstab

Die verfassungsrechtlichen Grenzen von Informationssystemen wurden in der Rechtsprechung des angerufenen Gerichts bislang nicht umfassend geklärt.

Die Entscheidungen zur *Bevorratung von Telekommunikationsdaten*,

BVerfGE 125, 260; 130, 151,

und die Urteile zur *Antiterrordatei*,

BVerfGE 133, 277; 156, 11,

betrafen Datenbestände, die jeweils erhebliche Besonderheiten aufwiesen. Die bevorrateten Telekommunikationsdaten fielen nicht im Rahmen der staatlichen Aufgabenerfüllung an, sondern waren anlasslos zu bevorraten. Darüber hinaus wurden diese Daten nicht bei Behörden, sondern bei Telekommunikationsunternehmen gespeichert. Die Antiterrordatei unterscheidet sich als Indexdatei, die sich auf einen spezifischen Sachbereich beschränkt und primär Datenübermittlungen vorbereitet, beträchtlich von breiter angelegten, in erster Linie für unmittelbare Auswertungen vorgesehenen Verbunddateien.

Im Übrigen standen im Vordergrund der Rechtsprechung die Anforderungen an die sich unmittelbar an die Erhebung anschließende zweckändernde Nutzung oder Übermittlung der Daten, die eine Behörde im Rahmen ihrer Aufgabenerfüllung erhoben hat.

Vgl. zuletzt BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 229 ff.

Anhand von Einzelaussagen aus der Rechtsprechung des angerufenen Gerichts und daneben – im Sinne von Rechtserkenntnisquellen – orientiert an der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Art. 8 EMRK und des Gerichtshofs der Europäischen Union zu Art. 7 und Art. 8 GRCh sowie an der JI-RL, lassen sich nichtsdestotrotz gewisse Grundsätze erkennen, die auch bei der Beurteilung des nachrichtendienstlichen Informationssystems Relevanz erlangen.

Um die Speicherung nachrichtendienstlicher Daten in verfahrensexternen Informationssystemen und die Nutzung der gespeicherten Daten in späteren Verfahren verfassungsrechtlich einzuhegen, bedarf es eigenständiger Maßstäbe. Insbesondere kann nicht ohne weiteres auf die grundrechtlichen Anforderungen an die unmittelbare Weiterverarbeitung erhobener Daten zurückgegriffen werden. Zwar werden in beiden Fallkonstellationen Daten aus dem Verfahren, in dessen Rahmen sie erhoben wurden, in weitere Verfahren überführt. Jedoch unterscheiden sich die beiden Fallkonstellationen darin, dass bei der unmittelbaren Weiterverarbeitung ein konkretes Zielverfahren bereits läuft oder mit der Weiterverarbeitung in Gang gesetzt wird, während zum Zeitpunkt der Datenspeicherung in einem Informationssystem noch nicht absehbar ist, ob, wann und in welchem Kontext die gespeicherten Daten einmal genutzt werden sollen.

Die Regulierung von Informationssystemen hat darum einen zeitlich gestreckten zweiaktigen Vorgang zum Gegenstand, der aus der Speicherung und der späteren Nutzung von Daten besteht. Hieraus ergeben sich praktische Verarbeitungsbedürfnisse, die bei der unmittelbaren Weiterverarbeitung von Daten nicht auftreten und darum bei der verfassungsrechtlichen Maßstabsbildung nicht berücksichtigt werden müssen. Zudem erzeugt die zeitliche Streckung von Datenbevorratung und Datennutzung besondere grundrechtliche Risiken, die durch besondere verfassungsrechtliche Anforderungen abgeschirmt werden müssen. Zugleich dürfen die Anforderungen an Informationssysteme nicht dazu führen, dass die Voraussetzungen von unmittelbaren Weiterverarbeitungen ausgehebelt werden. Diesbezüglich unterscheidet das angerufene Gericht zwischen zwei Weiterverarbeitungskonstellationen, für die es unterschiedlich

strenge verfassungsrechtliche Maßstäbe entwickelt hat, die für die Entwicklung eines eigenständigen Maßstabs für das Informationssystem herangezogen werden können.

a) Anforderungen an die Weiterverarbeitung von Daten

Eine Weiterverarbeitung erhobener Daten in einem Verfahren derselben Behörde im Rahmen derselben Aufgabe zum Schutz gleichwertiger Rechtsgüter wie im Ausgangsverfahren hält sich als weitere Nutzung im Rahmen der verfassungsrechtlichen Zweckbindung der Daten. Der Gesetzgeber darf eine solche weitere Nutzung unabhängig von weiteren gesetzlichen Voraussetzungen zulassen, solange die erhobenen Daten für eine neues Verfahren im Rahmen der ursprünglichen Erhebungszwecke einen hinreichenden Spurenansatz bilden.

> BVerfGE 141, 220 <325 Rn. 278>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 227.

Besondere Anforderungen ergeben sich jedoch bei Daten, die mittels Wohnraumüberwachungen und Online-Durchsuchungen erlangt wurden. Bei diesen bedarf es für jede weitere Nutzung in neuen Verfahren einer den Erhebungsvoraussetzungen entsprechend dringenden beziehungsweise zumindest konkretisierten Gefahr.

> BVerfGE 141, 220 <326 Rn. 283>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 228.

Hingegen ist eine Weiterverarbeitung durch eine andere Behörde oder durch dieselbe Behörde im Rahmen einer anderen Aufgabe als Zweckänderung besonders rechtfertigungsbedürftig. Der Gesetzgeber darf die zweckändernde Weiterverarbeitung nach dem Kriterium einer hypothetischen Datenneuerhebung zulassen, wenn der neue Verarbeitungszweck dem Erhebungszweck gleichwertig ist.

> BVerfGE 141, 220 <326 f. Rn. 284>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 229 ff.

b) Anforderungen an ein umfassendes Informationssystem

Aus den vom angerufenen Gericht entwickelten Maßstäben der Zweckbindung und Zweckänderung ergeben sich auch die äußeren Grenzen eines Informationssystems. Dieses darf weder Anforderungen stellen, die eine weitere Nutzung unmöglich machen würden. Noch dürfen die entsprechenden Anforderungen derart ausgestaltet sein, dass die Voraussetzungen der hypothetischen Datenneuerhebung dadurch umgangen werden könnten.

Auch darüber hinaus lassen sich Maßgaben ableiten. Hierzu sind im ersten Schritt die beiden Grundrechtseingriffe zu differenzieren, die mit der Führung eines Informationssystems einhergehen: die Speicherung und die spätere Nutzung von Daten.

Hinsichtlich der Speicherung von Daten sind für die materielle grundrechtliche Bewertung erstens der Inhalt des Informationssystems, der durch Art und Umfang der gespeicherten Daten bestimmt wird, sowie zweitens die Voraussetzungen und zeitlichen Grenzen einer Datenspeicherung maßgeblich.

Hinsichtlich der späteren Nutzung der gespeicherten Daten bilden erstens die Voraussetzungen und zulässigen Ziele einer Nutzung und zweitens die zulässigen Nutzungsarten die relevanten Faktoren.

> Vgl. zur Antiterrordatei für die Parameter Voraussetzungen der Speicherung (= erfasster Personenkreis), Inhalt der Datensammlung sowie Nutzungsvoraussetzungen und Nutzungsarten BVerfGE 133, 277 <339 ff., 350 ff., 360 ff.>; ferner EGMR, Urteil vom 13. November 2012, No. 24029/07 (M.M./Vereinigtes Königreich), Rn. 195; EGMR, Urteil vom 24. Januar 2019, No. 43514/15 (Catt/Vereinigtes Königreich), Rn. 95.

Allerdings können die beiden Grundrechtseingriffe nicht durchgängig separat voneinander betrachtet werden, vielmehr sind die beschriebenen vier Parameter aus grundrechtlicher Sicht miteinander verflochten. Die Eingriffe sind aufeinander bezogen, da die Anforderungen an die Datennutzung zugleich den Zweck der Datenspeicherung mitdefinieren. Die Eingriffsintensität des Informationssystems und die daraus folgenden grundrechtlichen Maßstäbe lassen

sich darum nur in einer Gesamtschau von Datenspeicherung und Datennutzung ermitteln.

> Vgl. für die Weiterverarbeitung BVerfGE 110, 33 <47> m.w.N. sowie ansatzweise EGMR, Urteil vom 13. November 2012, No. 24029/07 (M.M./Vereinigtes Königreich), Rn. 200.

Folglich stehen die Parameter der Regulierung von Informationssystemen zueinander in einem partiellen wechselseitigen Kompensationsverhältnis. Wird einer von ihnen weit gefasst, so müssen restriktivere Anforderungen an die anderen gestellt werden, um das Informationssystem insgesamt zu rechtfertigen und eine Balance herzustellen. Die Kompensation hat allerdings Grenzen. Insbesondere darf keiner der Parameter vollständig entgrenzt werden.

Soll etwa ein Informationssystem in großem Umfang sensible Daten enthalten, die unter niedrigen Voraussetzungen gespeichert werden, und ermöglicht das Gesetz ein breites Spektrum von Datennutzungen, so sind an die Voraussetzungen und Ziele der Datennutzung besonders strenge Anforderungen zu stellen.

> Vgl. für die Nutzung anlasslos bevorrateter Telekommunikations-Verkehrsdaten – insoweit hinsichtlich der Billigung einer anlasslosen Datensammlung allerdings mittlerweile überholt – BVerfGE 125, 260 <327 ff.>; für eine merkmalbezogene Recherche in der Antiterrordatei und für die umfassende Auswertung dieser Datei in Eilfällen BVerfGE 133, 277 <363 ff. >.

Wird die Nutzung solcher Daten eng auf weniger eingriffsintensive Nutzungsarten begrenzt, so können die Voraussetzungen und Ziele der Datennutzung offener formuliert werden.

> Vgl. für die Auflösung einer dynamischen IP-Adresse mittels bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 <340 ff.>; für die Nutzung der Antiterrordatei als Indexdatei BVerfGE 133, 277 <360 ff.>.

Daneben können großzügigere Regelungen für Art, Voraussetzungen und Ziele der Datennutzung gerechtfertigt werden, wenn sich der Inhalt eines Informationssystems auf einen begrenzten Bestand weniger sensibler Daten beschränkt, oder wenn die Datenbevorratung an besonders strenge Voraussetzungen geknüpft wird.

> Vgl. für die Nutzung bevorrateter Telekommunikations-Bestandsdaten BVerfGE 130, 151 <195 ff.>.

Allerdings bestehen verfassungsrechtliche Mindestanforderungen, die durch die wechselseitige Kompensation der Parameter nicht verschoben werden können.

(1) Mindestanforderungen an die Datenspeicherung

Auf der Ebene der Datenspeicherung ist den spezifischen Risiken Rechnung zu tragen, welche die Speicherung für die betroffenen Personen mit sich bringt. So kann die Speicherung unabhängig von den Anforderungen an die spätere Datennutzung eine Stigmatisierung der betroffenen Personen bewirken und Einschüchterungseffekte hervorrufen.

> Vgl. EGMR, Urteil vom 4. Dezember 2008, No. 30562/04 and 30566/04 (S. und Marper/Vereinigtes Königreich), Rn. 121 ff.

Zwar ist ein derartiges Risiko bei nachrichtendienstlichen Informationssystemen teilweise dadurch reduziert, dass die Datenerhebung und Speicherung in der Regel heimlich erfolgen. Zugleich intensiviert diese Heimlichkeit das Gewicht einer Speicherung, da diese verhindert oder erschwert, dass Personen dagegen vorgehen können, dass ihre Daten in einem Informationssystem vorgehalten werden.

> Zur Schwere heimlicher Eingriffe zuletzt BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 132.

Zudem birgt die Speicherung die nie auszuschließenden Risiken einer irrtümlich oder sogar missbräuchlich rechtswidrigen Nutzung der bevorrateten Daten und eines unbefugten Zugriffs auf die Daten durch Dritte.

> Vgl. beispielhaft zu einem derartigen Missbrauchsfall zulasten der Beschwerdeführerin zu 1 schwerwiegenden Missbrauchsfall bei einer Landespolizeibehörde: Frankfurter Anwältin erhält vierten Drohbrief von „NSU 2.0“, Zeit vom 5. Februar 2019, abrufbar unter https://www.zeit.de/politik/deutschland/2019-02/seda-basay-yildiz-drohbrief-frankfurter-rechtsanwaeltin-rechtsextremismus. Siehe bspw. auch BT-Drs. 20/2493; Polizisten missbrauchen Datenbank zum Ausspähen, Berliner Morgenpost vom 23. Juni 2022, abrufbar unter https://www.morgenpost.de/berlin/article235699371/Polizisten-missbrauchen-Datenbank-zum-Ausspaehen.html.

Insbesondere die anlasslose großflächige Speicherung sensibler Daten lässt sich deshalb unabhängig von den Modalitäten und Voraussetzungen der späteren Datennutzung nie rechtfertigen.

> Vgl. EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19 (PNR), Rn. 85 ff.; EuGH, Urteil vom 21. Dezember 2016, Rs. C 203/15 und C-698/15 (Tele2 Sverige u.a.), Rn. 97 ff.; EuGH, Gutachten 1/15 vom 26. Juli 2017, Rn. 204 ff.; tendenziell gleichläufig EGMR, Urteil vom 4. Dezember 2008, No. 30562/04 and 30566/04 (S. und Marper/Vereinigtes Königreich), Rn. 119 ff.; EGMR, Urteil vom 13. November 2012, No. 24029/07 (M.M./Vereinigtes Königreich), Rn. 195 ff.; überholt ist insoweit BVerfGE 125, 260 <316 ff.>.

Die Speicherung sensibler Daten ist vielmehr stets an einen zumindest ansatzweise konturierten Anlass zu knüpfen, der das Ausmaß der Datenspeicherung auf hinreichend gewichtige Fälle begrenzt.

> Vgl. EGMR, Urteil vom 18. April 2013, No. 19522/09 (M.K./Frankreich), Rn. 38; aus der Rechtsprechung des angerufenen

Gerichts BVerfGE 103, 21 <34>; BVerfG(K), Beschluss vom 16. Mai 2002 – 1 BvR 2257/01, Rn. 14 f.

Bloße Mutmaßungen über die betroffene Person oder lediglich vage Anhaltspunkte für ein Fehlverhalten reichen demgegenüber nicht aus, um solche Daten über einen längeren Zeitraum zu speichern.

Vgl. EGMR, Urteil vom 18. Oktober 2011, No. 16188/07 (Khelili/Schweiz), Rn. 63 ff.; aus der Rechtsprechung des angerufenen Gerichts BVerfGE 103, 21 <37>; BVerfG(K), Beschluss vom 1. Juni 2006 – 1 BvR 2293/03, Rn. 15.

Zudem muss zum Zeitpunkt der Speicherung zumindest ansatzweise absehbar sein, dass die bevorrateten Daten zukünftig einen Beitrag zur Aufgabenerfüllung erbringen können. Ist dies nicht der Fall, so ist die – auch unionsrechtlich durch Art. 4 Abs. 1 lit. c und e JI-RL vorausgesetzte – Erforderlichkeit der Bevorratung nicht gewährleistet.

Vgl. EGMR, Urteil vom 24. Januar 2019, No. 43514/15 (Catt/Vereinigtes Königreich), Rn. 116 ff.

Schließlich muss die Ermächtigung die Speicherung zeitlich begrenzen. Dies ist insbesondere bedeutsam, wenn die Speicherung an die Feststellung oder gar lediglich an den Verdacht oder die Prognose eines Fehlverhaltens der betroffenen Person anknüpft. Denn eine solche Datenspeicherung ist geeignet, stigmatisierende Wirkungen zu entfalten, die gerade nach längerer Zeit die betroffene Person unangemessen belasten können.

Vgl. EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19 (PNR), Rn. 248 ff.; EGMR, Urteil vom 4. Dezember 2008, No. 30562/04 and 30566/04 (S. und Marper/Vereinigtes Königreich), Rn. 119; EGMR, Urteil vom 13. November 2012, No. 24029/07 (M.M./Vereinigtes Königreich), Rn. 199.

Dementsprechend schreibt Art. 5 JI-RL vor, dass für die Löschung von personenbezogenen Daten oder die regelmäßige Überprüfung der Notwendigkeit

ihrer Speicherung angemessene Fristen vorzusehen sind. Zudem ist durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

(2) Mindestanforderungen an die Datennutzung

Auf der Ebene der Datennutzung ist unabhängig von den Voraussetzungen der Datenbevorratung die grundrechtliche Zweckbindung zu beachten. Aus der zeitlichen Ausdehnung der Weiterverarbeitung ergibt sich kein Grund, von diesem Maßstab zulasten der betroffenen Person abzurücken. Zudem darf die zweckändernde Nutzung der Daten, welche Nachrichtendienste mit eingriffsintensiven Mitteln erhoben haben, nur zugelassen werden, wenn die Voraussetzungen einer hypothetischen Datenneuerhebung vorliegen.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 230 ff.

Bei Datennutzungen mit hoher Eingriffsintensität sind zudem besondere Anforderungen zu stellen, um diese Eingriffsintensität zu kompensieren.

> Vgl. für die erweiterte Datennutzung (Data-Mining) BVerfGE 156, 11 <52 ff. Rn. 107 ff.>.

Hingegen lässt sich die Rechtsfigur der weiteren Nutzung – die keine Zweckänderung darstellt – nicht ohne Weiteres auf die Nutzung von Daten übertragen, die über einen längeren Zeitraum gespeichert werden. Ansonsten würde die Nutzung dieser Daten während der potenziell langjährigen Speicherzeit im Rahmen der betreffenden behördlichen Aufgabe anlasslos ermöglicht und so ins Belieben der speichernden Behörde gestellt. Von der grundrechtlichen Zweckbindung bliebe im Rahmen der betreffenden Aufgabe ebenso wenig übrig wie von dem Gebot einer verhältnismäßigen Datenverarbeitung, obwohl beide durch Art. 4 Abs. 1 lit. b) und c), Abs. 2 JI-RL auch unionsrechtlich vorgegeben sind. Die weitere Nutzung bevorrateter Daten im Rahmen derselben behördlichen Aufgabe bedarf daher eines tatsächlichen Anlasses, wenngleich dieser schwächer konturiert ausfallen kann als die im Rahmen einer hypothetischen Datenneuerhebung erforderlichen Voraussetzungen.

3. Materielle Verfassungswidrigkeit

Das nachrichtendienstliche Informationssystem wird diesen Anforderungen nicht gerecht.

Bereits die Anforderungen an Speicherungen sind äußerst weitreichend angelegt und stellen für sich genommen einen verfassungsrechtlichen Verstoß dar (hierzu **a)**). Hinzu kommen extensive Regelungen zur Datennutzung (hierzu **b)**) und unzureichende Verfahrensregelungen (hierzu **c)**). Dementsprechend stellt auch das Informationssystem insgesamt einen unverhältnismäßig intensiven Grundrechtseingriff dar (hierzu **d)**).

a) Extensiver Umfang an gespeicherten Daten

(1) Inhalt des Informationssystems

Das nachrichtendienstliche Informationssystem ist von einem erheblichen Umfang geprägt, der jegliche Art von Daten umfasst.

So grenzt § 6 BVerfSchG nicht ein, welche Art von Dateien im Informationssystem gespeichert werden können. Vielmehr stellt § 6 Abs. 1 Satz 1 BVerfSchG explizit klar, dass auch die Erkenntnisse der Auswertungen der Nachrichtendienste zu speichern sind. Umfasst sind neben den Ergebnissen der nachrichtendienstlichen Analysetätigkeit auch Rohdaten wie „Freitexte, beliebige weitere Dokumente, Bilder, Videodateien oder sonstige Dateianhänge“.

> *Bergemann*, in: Lisken/Denninger PolR-HdB, 7. Aufl. 2021, H. Nachrichtendienste und Polizei Rn. 118. Siehe auch *ders.*, NVwZ 2015, 1705 (1705)); vgl. *Siems*, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 1. Aufl. 2017, § 7 Rn. 61.

Damit unterscheidet sich das nachrichtendienstliche Informationssystem erheblich von Indexsystemen, bei denen nur einzelne Informationen mit einem Verweis auf den Ort weiterer Information gespeichert werden. In einem derartigen Indexsystem ist also nicht die relevante Information selbst einsehbar,

sondern lediglich, bei welcher Behörde nach den weiteren Informationen zu fragen ist. Ein solches System – das früher auch zwischen den Nachrichtendiensten verwendet wurde – war insbesondere Gegenstand der Entscheidung des erkennenden Gerichts in seiner Entscheidung zum *Antiterrordateigesetz I*. Demnach stellt eine derartige Indexdatenbank einen verminderten Grundrechtseingriff dar.

> BVerfGE 133, 277 <329 ff. Rn. 124 ff.>.

Im Gegensatz dazu werden beim nachrichtendienstlichen Informationssystem Dateien direkt und vollumfänglich eingestellt, sodass diese auch direkt abgerufen werden können. Hierdurch entfällt jegliche zwischenbehördliche Kontrolle. Mit der vorhandenen Volltextsuche besteht daher ein erheblicher Grundrechtseingriff, gegen den sich auch die Datenschutzbeauftragten des Bundes und der Länder explizit ausgesprochen hatten.

> Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010, Keine Volltextsuche in Dateien der Sicherheitsbehörden.

Zudem wird dadurch die Trennung zwischen Personen- und Sachakten faktisch abgeschafft, die selbst eine eingriffsbegrenzende Funktion hat. Nach diesem System werden eingriffsintensive Personenakten, die vollumfängliche Informationen zu einer Person enthalten, nur ab einem gewissen Grad der Einbindung in eine Bestrebung angelegt.

> Vgl. *Bergemann*, in: Lisken/Denninger PolR-HdB, 7. Aufl. 2021, H. Nachrichtendienste und Polizei Rn. 109; *ders.*, NVwZ 2015, 1705 (1706).

Sachakten haben hingegen keine derartige Begrenzung und können auch Informationen zu Personen enthalten, zu denen keine Personenakten angefertigt werden dürfen.

> Vgl. *Bundesamt für Verfassungsschutz*, Im Visier des Verfassungsschutzes – Der gläserne Bürger?, 2013, S. 18.

Dazu gehören Personen, bei denen keine derartige Einbindung vorliegt. Gesetzliche Einschränkungen bestehen auch bei den Daten von Minderjährigen, § 11 Abs. 2 BVerfSchG.

> *Bergemann*, in: Lisken/Denninger PolR-HdB, 7. Aufl. 2021, H. Nachrichtendienste und Polizei Rn. 108; Bundesbeauftragter für Datenschutz und die Informationsfreiheit, 23. Tätigkeitsbericht zum Datenschutz für die Jahre 2009 - 2010, 2011, S. 92.

Da in das nachrichtendienstliche Informationssystem beide Arten von Akten eingepflegt werden, entfällt dieser Schutz faktisch, da im Informationssystem alle vorhandenen Informationen anhand einer Freitextsuche aufgefunden werden können.

Bezüglich der Art der gespeicherten Daten liegt damit der weitestmögliche Eingriff.

> Vgl. *Bergemann*, NVwZ 2015, 1705 (1706).

Jedenfalls aber bedarf es erheblicher Kompensationen durch die anderen Parameter des Informationssystems.

(2) Voraussetzungen und Grenzen der Speicherpflicht

Die Voraussetzungen und Grenzen der Speicherpflicht sind äußerst niedrig angelegt.

(a) Geringer Speicheranlass „Relevanz“

Nach § 6 Abs. 1 Satz 1 BVerfSchG besteht die Übermittlungs- und damit Speicherpflicht bei sämtlichen „relevanten Informationen“. Das Anknüpfungsmerkmal der Relevanz ersetzt damit den sonst üblichen Maßstab der Erforderlichkeit, der bezüglich der Übermittlungspflichten dem MAD weiterhin gilt, § 3 Abs. 3 Satz 1 MADG.

Damit liegt eine Absenkung der Eingriffsschwelle vor,

Siehe bereits BR-Drs. 123/15, S. 27. Siehe auch *Bergemann*, NVwZ 2015, 1705 (1706).

Der Begriff der relevanten Informationen wird dementsprechend so ausgelegt, dass sämtliche Informationen zu übermitteln sind, die möglicherweise erheblich sind.

Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG, § 6 Rn. 9 m.w.N.

Die übermittelnde Behörde prüft dies lediglich in summarischer Weise und übermittelt jegliche Informationen, die nicht offensichtlich unerheblich sind – also auch, wenn Zweifel hinsichtlich der Relevanz bestehen.

Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG, § 6 Rn. 10 f. m.w.N.

Auch bei Zweifeln hinsichtlich der Richtigkeit von Informationen sind diese zu übermitteln, allerdings mit einer entsprechenden Kennzeichnung.

Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG, § 6 Rn. 12 m.w.N.

Damit besteht praktisch kaum eine Eingrenzung des Umfangs der zu speichernden Daten. Vielmehr wird dadurch bewirkt, dass Informationen, die bei einer Behörde gespeichert werden, weitgehend auch mit allen anderen Behörden geteilt werden können.

In Bezug auf den MAD findet eine gewisse Einschränkung statt. So umfasst die Übermittlungspflicht zwischen dem MAD und den Verfassungsschutzbehörden lediglich erforderliche Informationen § 3 Abs. 3 Satz 1 MADG.

Diese Hürde gilt allerdings nur noch teilweise, sobald der MAD am Informationssystem teilnimmt. Dann hat zumindest dieser Zugriff auf sämtliche Informationen, die dort aufgrund des Merkmals Relevanz eingespeist wurden. Die höhere Hürde wirkt sich dadurch nur auf die vom MAD übermittelten Informationen aus.

Etwas anderes ergibt sich auch nicht durch den in § 6 Abs. 2 Satz 4 BVerfSchG enthaltenen Verweis auf §§ 10 und 11 BVerfSchG. Zwar schränkt § 10 Abs. 1 BVerfSchG auch ein, unter welchen Umständen Daten gespeichert werden dürfen. Es ist aber nicht davon auszugehen, dass der Verweis auch die Speicherung im Informationssystem umfasst. So spricht § 6 Abs. 2 Satz 4 BVerfSchG von der Verarbeitung *im* nachrichtendienstlichen Informationssystem. Obgleich der Begriff der Verarbeitung nach gängiger Definition auch die Speicherung umfasst, spricht der Wortlaut doch dafür, dass es sich um Daten handeln muss, die sich bereits im System befinden.

Dafür spricht auch, dass der Verweis auf die §§ 10 und 11 BVerfSchG erst im Zusammenhang mit der Ausweitung des Informationssystems um den MAD eingefügt wurde. Das Kriterium der Relevanz galt aber bereits zuvor. Die Gesetzesbegründung begreift den neu eingefügten Verweis aber nicht als Eingrenzung der Speicherpflicht.

> BT-Drs. 19/24785, S. 18.

Jedenfalls kann nicht davon ausgegangen werden, dass § 10 Abs. 1 BVerfSchG als Einschränkung des Relevanzkriteriums den verfassungsrechtlichen Bestimmtheitsanforderungen gerecht werden würde.

§ 10 Abs. 1 BVerfSchG und vergleichbare Landesregelungen (vgl. etwa § 7 LVSG BaWü, § 8 VSG NRW, § 9 HmbVerfSchG) führen zudem nicht dazu, dass bereits auf Erhebungsebene eine hinreichende Einschränkung vorliegt, welche auch auf die Übermittlungspflicht nach § 6 Abs. 1 BVerfSchG durchschlägt. So umfasst § 10 Abs. 1 BVerfSchG – neben den weiten Speichermöglichkeiten aufgrund tatsächlicher Anhaltspunkte für Bestrebungen und der Erforschung und Bewertung von Bestrebungen (Nr. 1 und 2) – auch die Speicherung von Daten aus Sicherheits- und anderen Überprüfungen durch den Verweis auf § 3 Abs. 2 BVerfSchG (Nr. 3). Damit dürfen weitgehend alle Daten aus dem Aufgabenfeld der Nachrichtendienste auch gespeichert werden. Lediglich Daten aus Maßnahmen, die ihr Ziel verfehlt haben, sind nicht erfasst. Dies erscheint grundsätzlich auch sachgerecht; wenn den Nachrichtendiensten Überwachungsbefugnisse zugestanden werden, dürfen diese die Erkenntnisse daraus

auch speichern, sofern sich nützliche Informationen ergeben haben. Davon zu trennen ist aber die Frage, unter welchen Umständen diese Informationen zugleich auch mit anderen Nachrichtendiensten geteilt werden können.

Das hierfür geforderte Kriterium der Relevanz ist unzureichend. Faktisch besteht aufgrund des weiten Verständnisses des Kriteriums nahezu keine Eingriffsschwelle. Eine solche ist aber auch bei der Speicherung von Dateien in einer gemeinsamen Datenbank verfassungsrechtlich geboten.

(b) Keine Beschränkung des Personenkreises

Unabhängig von dessen unmittelbarer Anwendbarkeit ergibt sich aus § 10 Abs. 2 Satz 1 BVerfSchG, dass im nachrichtendienstlichen Informationssystem grundsätzlich keine Einschränkungen hinsichtlich der Speicherung von personenbezogenen Daten Dritter vorgesehen sind. Dabei handelt es sich um Personen, die selbst nicht – auch nicht als Randperson – Anlass zu einer nachrichtendienstlichen Maßnahme gegeben haben, sondern lediglich in irgendeiner Verbindung zu Zielpersonen oder Sachverhalten stehen. Das können beispielsweise Nachbar*innen, Kolleg*innen und Familienmitglieder sein. Der Umstand, dass über diese Informationen gespeichert werden, obwohl sie selbst keinen Anlass dafür gegeben haben, stellt nach der Rechtsprechung des angerufenen Gerichts einen intensiven Grundrechtseingriff dar.

> Vgl. BVerfGE 109, 279 <351, 352 Rn. 254, 255, 294, 297>; 120, 274 <329, 334 Rn. 233>; 113, 348 <382 f. Rn. 140>; 141, 220 <273 f., Rn. 115>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 211.

§ 10 Abs. 2 Satz 2 BVerfSchG gibt zwar vor, dass Daten Dritter nicht abgefragt werden dürfen. Im Umkehrschluss bedeutet dies jedoch, dass Daten Dritter zunächst sehr wohl gespeichert werden dürfen. Die Einschränkung gilt mithin nur bezüglich einer anschließenden Abfrage, also einer weiteren Datennutzung (hierzu **D.V.2.a)**).

Eine Beschränkung hinsichtlich der Speicherung ergibt sich lediglich gegenüber Minderjährigen unter 14 Jahren, § 6 Abs. 2 Satz 4 i.V.m. § 11 Abs. 1 BVer-

fSchG. Aufgrund der hohen Eingriffsintensität ist jedoch eine weitergehende Beschränkung des Personenkreises erforderlich.

(c) Keine Beschränkung regionaler Aktivitäten

Relevante Information umfassen aufgrund der zentralen Auswertungsfunktion des BfV gemäß § 5 Abs. 2 BVerfSchG auch Informationen, die lediglich regionalen oder lokalen Bezug aufweisen.

> *Roth*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG, § 6 Rn. 9; *Bergemann*, NVwZ 2015, 1705 (1705).

Auch die Informationen über eine Bestrebung oder einen Sachverhalt, der damit eingrenzbar nur lokale Relevanz hat, sind mithin zu übermitteln. Das führt dazu, dass sämtliche Verfassungsschutzbehörden auch Zugriff auf derartige Informationen aus allen Ländern haben.

Die föderale Struktur der Verfassungsschutzbehörden enthält aber selbst auch eine freiheitsfördernde Dimension, da mit der bundesstaatlichen Staatsorganisation gem. Art. 20 Abs. 1 und Art. 28 GG zugleich eine Verhinderung übermäßiger staatlicher Machtkonzentration intendiert war.

> Vgl. *Härtel,* in: Härtel (Hrsg.), Handbuch Föderalismus, Bd. I, 2012, § 16 Rn. 41; *Uhle*, in: Dürig/Herzog/Scholz, GG, 96. EL November 2021, Art. 70 GG Rn. 11.

(d) Keine Beschränkung der Speicherung sensibler Dateien oder nach Eingriffsintensität der Erhebungsmaßnahme

Darüber hinaus findet keine Beschränkung dahingehend statt, dass besonders sensible Dateien oder solche Informationen, die durch besonders intensive Maßnahmen erlangt wurden, nur beschränkt in das Informationssystem aufzunehmen sind.

Zwar besteht bei sensiblen Dateien bereits ein gewisser Schutz durch diverse Regelungen zum Kernbereichsschutz. Aber auch über diesen Bereich hinaus

können Daten sensibel sein. Eine Abschichtung nach derartigen Daten sieht § 6 BVerfSchG nicht vor.

Auch wird nicht danach differenziert, welche Intensität die Erhebungsmaßnahme hatte. Damit können auch Daten gespeichert werden, die aus äußerst eingriffsintensiven Maßnahmen herrühren. Hierzu gehören beispielsweise Erkenntnisse aus Wohnraumüberwachung aber zugleich auch die Erkenntnisse aus einer Quellen-Telekommunikationsüberwachung oder einer Online-Durchsuchung.

Dies wird auch nicht durch andere Vorschriften des Bundesverfassungsschutzgesetzes eingeschränkt. So sieht § 9 Abs. 2 BVerfSchG Einschränkungen bei intensiven Erhebungen vor und verweist in diesem Zusammenhang auch auf § 4 Abs. 4 und 6 G 10. Das ist aber nicht ausreichend.

So ist bereits nicht davon auszugehen, dass die Vorschrift im Rahmen des Informationssystems Anwendung findet. § 6 BVerfSchG bezieht sich selbst nicht auf die Vorschrift. Auch nimmt § 4 Abs. 4 Satz 1 G 10 die Nachrichtendienste von den Übermittlungseinschränkungen durch den Verweis auf § 1 Abs. 1 Nr. 1 G 10 aus.

Darüber hinaus leidet § 4 Abs. 4 G 10 selbst an erheblichen Mängeln (hierzu **IV.**).

(e) Keine Einschränkung durch § 6 Abs. 1 Satz 2 BVerfSchG

Auch § 6 Abs. 1 Satz 2 BVerfSchG – nach dem sich Behörden vorbehalten können, dass Daten nur mit ihrer Zustimmung an Dritte übermittelt werden können – führt zu keiner Einschränkung der Intensität des Eingriffs durch die Speicherung der Daten.

Bei der Regelung handelt es sich lediglich um eine Umsetzung der *Third Party Rule*. Diese schränkt aber gerade nicht die Übermittlung gegenüber anderen Verfassungsschutzbehörden ein, sondern betrifft ausschließlich die Übermittlung außerhalb dieses Systems, also beispielsweise an das BSI (hierzu **III.3.b)(3)(b)(ii)**).

(3) Verfassungswidrigkeit der Speicherung

Damit stellt sich die Speicherverpflichtung des § 6 Abs. 1 Satz 1, Abs. 2 Satz 1 BVerfSchG, § 3 Abs. 3 MADG für sich genommen als unverhältnismäßig dar.

Sie statuiert eine Eingriffsermächtigung, die eine Speicherung von faktisch nahezu allen Dateien einer Verfassungsschutzbehörde in einem gemeinsamen System vorschreibt. Diese gemeinsame Speicherung der vollständigen Dateien, inklusive Auswertungen und Anhängen, ist ein erheblicher Grundrechtseingriff. Hinzu kommt, dass auch Informationen von Personen gespeichert werden, die selbst keinen Anlass dafür gegeben haben.

Diese Defizite können durch Einschränkungen auf der Nutzungsebene nicht mehr ausgeglichen werden. Vielmehr ist es notwendig, dass bereits auf Speicherebene gewisse Einschränkungen getroffen werden. Denn bereits durch die Speicherung entsteht die Gefahr, dass die Daten bewusst oder unbewusst durch die anschließende Datennutzung missbraucht werden könnten.

Darüber hinaus ist zu berücksichtigen, dass auch ein nicht zu unterschätzendes Risiko besteht, dass sich unbefugte Dritte Zugang zu den Daten verschaffen könnten. Denn es wird nicht deutlich, ob und welche Vorkehrungen zum Datenschutz – wie etwa eine Verschlüsselung – getroffen werden. In Anbetracht des erheblichen (finanziellen) Wertes personenbezogener Daten in der heutigen Zeit wird durch einen solch umfassenden Verbund an gespeicherten Daten ein erheblicher Anreiz geschaffen, sich unbefugten Zugang zu den Daten zu verschaffen.

Somit bedarf es eines Mindestmaßes an Einschränkungen auf der Speicherebene, die zumindest so weit gehen, dass jedenfalls eine vollkommen außer Verhältnis stehende Speicherung jeglicher Art von Daten nicht leichtfertig ermöglicht wird.

Eine solche Einschränkung ist jedoch beim Informationssystem der Nachrichtendienste nicht vorhanden. Das System könnte in seiner Reichweite kaum weiter sein. Es ermöglicht nicht nur, sondern verpflichtet sogar zur Speicherung, wenn nicht ausgeschlossen werden kann, dass die Daten für andere

Nachrichtendienste von Relevanz sein könnten. Da selbst Informationen zu regionalen Bestrebungen relevant sind, lässt sich kaum ein Fall erdenken, bei dem die Ersterhebungsbehörde berechtigt Daten erhoben hat, die diese dann nicht in das System einbringen müsste. Einschränkungen bestehen nur für die Erfassung von Daten Minderjähriger unter 14 Jahren.

Ein solch umfassendes Informationssystem birgt ein großes Missbrauchsrisiko auch durch kriminelle Dritte, insbesondere in Anbetracht der aktuellen großen Gefährdungslage der IT-Sicherheit, nicht zuletzt aufgrund des hohen (finanziellen) Wertes personenbezogener Daten (hierzu **III.2.a)**). Dieses Risiko wird auch durch die hohen Güter, die die Nachrichtendienste sichern sollen, nicht mehr gerechtfertigt. So ist es insbesondere unverhältnismäßig, dass das Informationssystem auch vollumfänglich Daten von Dritten enthalten darf. Diese haben kein Anlass für die Speicherung gegeben. Ihre Aufnahme kommt damit vielmehr einer Bevorratung von Daten nahe, die in aufgezeigter Weite nicht zulässig ist.

b) Extensive Nutzungsmöglichkeiten

Die Einschränkungen auf der Nutzungsebene vermögen die Schwächen auf der Speicherungsebene nicht einzudämmen.

(1) Voraussetzungen und zulässige Ziele einer Nutzung

(a) Nutzungsvoraussetzungen

Nach § 6 Abs. 2 Satz 4 i.V.m. § 10 Abs. 1 BVerfSchG sind Nutzungen möglich, wenn tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 BVerfSchG (Nr. 1) vorliegen, die Nutzung für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 BVerfSchG erforderlich ist (Nr. 2) oder das BfV nach § 3 Abs. 2 BVerfSchG tätig wird (Nr. 3)(hierzu gehören beispielsweise Sicherheitsüberprüfungen). Damit wird die Nutzung an die Aufgaben des BfV (und der Landesbehörden) geknüpft.

Mithin sind die Nutzungsvoraussetzungen nicht per se unzureichend, um Eingriffe zu rechtfertigen.

Problematisch ist aber, dass diese Anforderungen nicht danach differenzieren, auf welche Weise die Daten erhoben wurden. Im System können auch Informationen gespeichert sein, die durch eingriffsintensive Maßnahmen – wie die Quellen-Telekommunikationsüberwachung, die Online-Durchsuchung oder aber auch die Wohnraumüberwachung – erlangt wurden. Das führt insofern zu dem Problem, dass auf diese Daten auch zugegriffen werden kann, ohne dass die besonders strengen Voraussetzungen für derartige Maßnahmen weiterhin vorliegen.

Auch wenn beispielsweise keine Anhaltspunkte mehr dafür bestehen, dass eine Person eine Katalogstraftat des § 3 Abs. 1 Satz 1 G 10 planen würde, könnte weiterhin auf die im Informationssystem gespeicherten Daten aus einer beschränkten Online-Durchsuchung auch von anderen Behörden zugegriffen werden. Damit besteht die Gefahr der Umgehung der Eingriffsvoraussetzungen. Mithin wird dadurch dem Grundsatz der hypothetischen Datenneuerhebung für eine zweckändernde Nutzung (hierzu bereits **2.a)**) nicht ausreichend Rechnung getragen. Dementsprechende Vorgaben sind jedoch erforderlich und eine solche Umsetzung findet sich bereits in anderen Regelungen, wie beispielsweise in §§ 100e Abs. 6, 161 Abs. 3 und 479 Abs. 2 StPO.

Vgl. BVerfGE 141, 22 <327 f., Rn. 287>.

Eine derartige Einschränkung sehen die § 6 BVerfSchG und § 3 Abs. 3 MADG nicht vor.

(b) Keine hinreichende Beschränkung der Zielpersonen

Auch bei der Datennutzung sind wie bereits bei der Datenspeicherung die Voraussetzungen hinsichtlich der möglichen Zielpersonen zu weit gefasst. Eine Einschränkung hinsichtlich des Personenkreises, über den Informationen abgerufen werden können, ergibt sich zwar aus § 6 Abs. 2 Satz 4 i.V.m. § 10 Abs. 2 Satz 2 BVerfSchG. Danach können Daten Dritter nicht abgefragt werden.

Allerdings bewirkt diese Regelung keine hinreichende Einschränkung des Kreises an Personen, deren Daten ausgewertet werden können.

So ist bereits der Begriff des Dritten zu unbestimmt, um eine wirksame Begrenzung zu erzielen. Ein Dritter ist jedenfalls eine Person, die nicht von § 10 Abs. 1 BVerfSchG erfasst ist. Da diese Norm aber selbst keine hinreichende Umschreibung der Zielpersonen trifft, ist auch nicht hinreichend deutlich, wer Dritter sein kann.

> Vgl. *Bergemann*, in: Lisken/Denninger PolR-HdB, 7. Aufl. 2021, H. Nachrichtendienste und Polizei Rn. 54 ff.

Dies wäre aber insbesondere deswegen notwendig, da das gängige Verständnis möglicher Zielpersonen äußerst weit ist. Darunter fallen auch Randpersonen einschließlich Mitläufer*innen, Anscheinsaktivist*innen, Kontakt- und Begleitpersonen und darüber hinaus auch sogenannte „nützliche Idiot*innen", also undolose Helfer*innen.

> *Bergemann*, NVwZ 2015, 1705 (1706) m.w.N. Zur Reichweite von Randpersonen siehe auch BVerwG, Urteil vom 11. November 2004 – 3 C 8.04.

Dieser Personenkreis hat allerdings keinen, beziehungsweise einen nur geringen Anlass zur Datenauswertung gegeben. Bei diesen Personen besteht daher schon eine besondere Eingriffsintensität. Bei Dritten, also Personen, die nicht einmal einen derartigen Ermittlungsanlass gegeben haben, gilt dies umso mehr.

> Vgl. BVerfGE 109, 279 <351, 352 Rn. 254, 255, 294, 297>; 120, 274 <329, 334 Rn. 233>; 113, 348 <382 f. Rn. 140>; 141, 220 <273 f., Rn. 115>; BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 211.

Dabei ist zudem zu berücksichtigen, dass bereits auf der Speicherebene kein Schutz von Dritten erfolgt. Die Daten sind daher umfassend im Informationssystem vorhanden. Durch die Option der Volltextsuche sind diese auch ohne weiteres auffindbar. Dies ermöglicht die Nutzung von Daten einer Person, die

selbst nicht Ziel einer Erhebungsmaßnahme war oder sein durfte. Um diese Möglichkeit einzuschränken, bedarf es deshalb umso mehr hinreichend bestimmter Vorschriften, welcher Personenkreis Zielperson einer Datennutzung sein kann. Eine solch bestimmte Vorschrift sieht § 6 Abs. 2 Satz 4 i.V.m. § 10 Abs. 2 Satz 2 G 10 nicht vor.

(c) Keine hinreichende Einschränkung durch § 6 Abs. 2 Satz 3 BVerfSchG

Eine Einschränkung der Vorschrift folgt nicht aus § 6 Abs. 2 Satz 3 BVerfSchG, der auf die Regelungen §§ 22a und 22b BVerfSchG verweist. Aus der Formulierung „im Übrigen" ist ersichtlich, dass die Teilnahme am Informationssystem durch die Verfassungsschutzbehörden und den MAD durch die Vorschrift gerade nicht eingeschränkt werden soll. Nach der Gesetzesbegründung stellt die Vorschrift in diesem Sinne auch lediglich klar, „dass die speziellen gesetzlichen Regelungen für eine gemeinsame Datenhaltung zur Zusammenarbeit im nachrichtendienstlichen Bereich unberührt bleiben."

BT-Drs. 19/24785, S. 17.

Im Kern bedeutet dies also, dass für projektbezogene gemeinsame Dateien (§ 22a BVerfSchG) und die Errichtung gemeinsamer Dateien mit ausländischen Nachrichtendiensten (§ 22b BVerfSchG) weiterhin die Spezialvorschriften gelten. Eine Einschränkung des Informationssystems nach § 6 BVerfSchG findet damit aber nicht statt.

(d) Keine hinreichende Einschränkung durch § 6 Abs. 2 Satz 7 bis 9 BVerfSchG

Nach § 6 Abs. 2 Satz 7 bis 9 BVerfSchG bestehen bestimmte Einschränkungen dahingehend, welche Personen mit der Datenauswertung befasst sind. Konkret sind Abfragen nur für Personen möglich, für deren Aufgabenerfüllung eine solche Abfrage erforderlich ist (§ 6 Abs. 2 Satz 7 BVerfSchG). Ferner bestehen Beschränkungen auf Personen, die mit der Datenerfassung und Analyse betraut (§ 6 Abs. 2 Satz 8 BVerfSchG), sowie auf Personen, die mit den entsprechenden Anwendungsgebieten vertraut sind.

Hierbei handelt es sich in erster Linie um Zuständigkeitsregelungen.

> *Bergemann*, in: Lisken/Denninger PolR-HdB, 7. Aufl. 2021, H. Nachrichtendienste und Polizei Rn. 54 ff.

Insofern wird zwar der Personenkreis eingeschränkt, dem Informationen offenbart werden. Dies führt jedoch kaum zu einer relevanten Einschränkung. Bereits aus dem Eingriff in das Recht auf informationelle Selbstbestimmung folgt, dass nicht jede Person, die bei einer Verfassungsschutzbehörde beschäftigt ist, ohne Bezug zu ihren konkreten Aufgaben Zugriff auf das Informationssystem nehmen darf.

Darüber hinaus nennt § 6 Abs. 2 Satz 7 BVerfSchG zwar als Voraussetzung die Erforderlichkeit der Datennutzung, allerdings ist davon auszugehen, dass hierdurch keine über § 6 Abs. 2 Satz 4 i.V.m. § 10 Abs. BVerfSchG hinausgehende Einschränkung erfolgt. Bereits dort ist der Begriff der Erforderlichkeit angelegt, wenn auch nur in § 10 Abs. 1 Nr. 2 BVerfSchG. Zumindest aber stellt die Vorschrift keine hinreichend bestimmte Einschränkung dar. So ist aufgrund des Verweises in § 6 Abs. 2 Satz 4 G 10 davon auszugehen, dass der Maßstab des § 10 Abs. 1 BVerfSchG gilt. Wenn dieser zu modifizieren ist, wäre eine derartige Einschränkung in systematischer Nähe zu Satz 4 zu anzusiedeln, nicht aber erst in Satz 7 im Kontext von Zuständigkeitsregelungen.

(2) Zulässige Nutzungsarten

§ 6 Abs. 2 Satz 4 BVerfSchG i.V.m. § 10 Abs. 1 BVerfSchG ermöglicht die Nutzung der Dateien, ohne aber näher festzulegen, was dies überhaupt bedeutet. § 10 Abs. 1 BVerfSchG nennt als verschiedene Arten lediglich „verändern“ und „nutzen“ von Daten. Im Zusammenhang mit § 5 Abs. 2 Satz 1 BVerfSchG ergibt sich, dass eine derartige Nutzung auch die Auswertung umfasst.

Mangels weitgehender spezifischer Einschränkungen wurde teilweise vertreten, dass eine vollumfängliche Nutzung zulässig sei, die auch die erweiterte Datennutzung (Data-Mining) umfasst, bei der bereits vorhandene große Da-

tenbestände selbständig auf Zusammenhänge analysiert werden, um auf diesem Wege neue Erkenntnisse zu generieren.

> *Bergemann*, NVwZ 2015, 1705 (1705 f.). Zur erweiterten Datennutzung vgl. BVerfGE 156, 11 <40 Rn. 74>.

Auch die Gesetzesbegründung geht von umfangreichen Nutzungsmöglichkeiten aus.

> BT-Drs. 18/4654, S. 23 f.

Jedoch ist mit der Rechtsprechung des angerufenen Gerichts davon auszugehen, dass eine derartige erweiterte Datennutzung aufgrund des damit verbundenen intensiven Grundrechtseingriffs einer eigenständigen Ermächtigungsgrundlage bedarf, die an eine konkretisierte Gefahr für ein herausragendes öffentliches Interesse anknüpft.

> BVerfGE 156, 11 <55 Rn. 116 f.>.

Damit ist bei einer verfassungskonformen Interpretation der Norm davon auszugehen, dass eine derartige Nutzung nicht ermöglicht werden soll. Indem es der Gesetzgeber vollkommen offengelassen hat, was von „verändern und nutzen“ von personenbezogenen Daten konkret umfasst ist, hat er die Bedeutung und Tragweite der damit verbundenen Grundrechtseingriffe verkannt. Vor dem Hintergrund des erheblichen Umfangs der im Informationssystem zu speichernden Daten wäre es aber zwingend notwendig, hinreichend bestimmt festzulegen, welche Datennutzungen konkret möglich sind. Sollten dazu auch eingriffsintensivere Nutzungsarten zählen, müssten für diese gegebenenfalls strengere Voraussetzungen aufgestellt werden.

c) Keine hinreichenden Kontrollmöglichkeiten

Diese Defizite werden auch nicht durch Verfahrenssicherungen aufgefangen.

Dabei ist zunächst fraglich, welche Form von Verfahrenssicherungen überhaupt im Rahmen eines derart umfassenden Informationssystems zu fordern sind.

Aufgrund der Vielzahl an enthaltenen Informationen ist zweifelhaft, dass für ein derartiges System eine Benachrichtigungspflicht praktikabel sein kann.

> Vgl. BVerfGE 133, 277 <369>, wonach auch bei der Antiterrordatei keine Benachrichtigungspflichten zu fordern waren. Dies ist allerdings mit Verweis auf Ermittlungen im Bereich des internationalen Terrorismus zu unterstützen, die grundsätzlich nicht offen erfolgen könnten.

Ähnliche Zweifel bestehen hinsichtlich einer Individualrechtsschutzkontrolle im Sinne einer *ex ante* oder *ex post* Kontrolle jedweder Speicherungen oder Abrufen. Es ist kaum praktikabel, jede Information, die gespeichert oder genutzt wird, vorab zu kontrollieren. Zudem werden viele dieser Speicherungen und Nutzungen für sich betrachtet gegenüber den ursprünglichen Erhebungen nur ein geringfügiges weiteres Eingriffsgewicht erreichen.

> Vgl. BVerfGE 133, 277 <369>.

In Bezug auf das Antiterrordateigesetz forderte das angerufene Gericht insbesondere eine Protokollierungspflicht und ließ darüber hinaus eine datenschutzrechtliche Kontrolle genügen. Auch § 6 Abs. 3 i.V.m. § 28 Abs. 2 BVerfSchG knüpfen an eine derartige Datenschutzkontrolle an. Diese ist jedoch in mehrfacher Hinsicht ungenügend.

So ist bereits keine vollumfängliche datenschutzrechtliche Aufsicht möglich, da dieser gemäß §§ 15 Abs. 4 Satz 4, 28 Abs. 3 Satz 3 BVerfSchG Auskünfte aus Sicherheitsgründen verweigert werden können. Die Notwendigkeit dieser Beschränkung ist nicht ersichtlich, vielmehr könnte stattdessen mit Vertraulichkeitsregelungen gearbeitet werden. Gerade im Bereich der politischen Vorfeldaufklärung besteht die Gefahr, dass derartige Sicherheitsbedenken regelmäßig bestehen und damit die Kontrolle faktisch ausgehöhlt wird. Durch Vertraulichkeitsregelungen könnte jedoch sichergestellt werden, dass eine effektive Kontrolle erfolgt und zugleich Sicherheitsbedenken begegnet werden kann.

> Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 224, anders noch BVerfGE 133, 277 <371>.

Hinzu ist eine turnusmäßige Überprüfung zu fordern.

BVerfGE 133, 277 <371>.

Eine derartige Verpflichtung ist in § 6 Abs. 3 BVerfSchG jedoch nicht vorgesehen.

Aufgrund des besonderen Umfangs der im Informationssystem gespeicherten Daten ist zudem fraglich, ob überhaupt eine Kontrolle nur durch den Bundesbeauftragten für Datenschutz (und Landesbehörden) ausreichend ist, die sich von einer gerichtlichen Kontrolle erheblich unterscheidet.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 200.

Auch sind keine hinreichenden Löschpflichten vorgesehen. Zwar enthält § 6 Abs. 2 Satz 4 BVerfSchG, § 10 Abs. 3 BVerfSchG die Vorgabe, die Speicherdauer auf das „erforderliche Maß“ für die Aufgabenerfüllung zu beschränken. Da dies aber von der Behörde aufgrund des weiten Bereichs der Aufgabenwahrnehmung selbst festgelegt wird, ergeben sich daraus kaum hinreichend bestimmte Beschränkungen. Verfassungsrechtlich vorzugswürdig wäre eine konkrete Einschränkung, die bestimmte Löschfristen mit Ausnahmeregelungen vorsieht.

Eine derartige Löschfristenregelung ist lediglich für die Daten von Minderjährigen vorgesehen, § 6 Abs. 2 Satz 4 BVerfSchG i.V.m. § 11 Abs. 3 BVerfSchG. Damit wird deutlich, dass eine derartige Regelung auch im Bereich eines Informationssystems möglich ist. Dann besteht aber kein Grund, diese Regelung nicht auch generell anzuwenden.

Zudem ist unklar, inwieweit § 10 Abs. 3 BVerfSchG in diesem Kontext überhaupt Anwendung findet. Da hier der Maßstab der Erforderlichkeit – zumindest begrifflich – verwendet wird, deckt sich der verwendete Maßstab nicht mit der Übermittlungspflicht des § 6 Abs. 1 BVerfSchG. Daher müssten Daten bereits wenn diese relevant sind übermittelt werden, dann aber gelöscht werden, wenn sie nicht erforderlich sind. Um diesen Widerspruch aufzulösen ist, wohl davon auszugehen, dass auch im Rahmen der Löschpflicht der Maßstab

der Relevanz anzuwenden ist. Dieser bewirkt aber kaum eine Eingrenzung der zu speichernden Daten.

Jedenfalls ist damit nicht hinreichend bestimmt, nach welchem Maßstab eine Löschung zu erfolgen hat.

d) Verfassungswidrigkeit des Informationssystems insgesamt

Es ist davon auszugehen, dass bereits die Regelungen zur Speicherung für sich genommen über das verfassungsrechtlich Mögliche hinausgehen.

Jedenfalls aber stellt sich das Gesamtsystem als zu weitgehend dar, als dass es noch mit dem Recht auf informationelle Selbstbestimmung im Einklang stehen könnte.

So wird das System maßgeblich dadurch bestimmt, dass faktisch nahezu alle Informationen der einzelnen Verfassungsschutzbehörden in das gemeinsame Informationssystem übertragen werden.

Diese Weite wird nicht hinreichend durch die Einschränkungen auf Nutzungsebene kompensiert. Zwar werden zunächst Eingriffsschwellen für eine Nutzung festgelegt, die vor dem Hintergrund nachrichtendienstlicher Tätigkeit nicht grundsätzlich zu kritisieren sind. Jedoch sind die Eingriffsschwellen dadurch defizitär, dass sie unabhängig davon gelten, durch welche Art von Eingriff die Informationen erlangt wurden. Darüber hinaus bestehen auch keine hinreichend bestimmten Regelungen, welche Arten der Nutzung ermöglicht werden sollen. Schließlich ist nicht hinreichend klar bestimmt, wer Zielperson einer Datennutzung werden kann. Dies ist insbesondere vor dem Hintergrund problematisch, dass auch Daten Dritter vollumfänglich im Informationssystem gespeichert werden und diese Daten durchsuchbar sind.

Darüber hinaus unterliegen Nutzungen lediglich einer datenschutzrechtlichen Kontrolle, die in ihrer konkreten Ausgestaltung ungeeignet ist, um die schwerwiegenden Grundrechtseingriffe und fehlenden Verfahrenssicherungen hinreichend zu kompensieren. Zudem bestehen keine hinreichend Löschregelungen.

Im Ergebnis liegt damit ein System vor, in dem umfangreiche Daten gespeichert werden, ohne dass die Nutzung der Daten hinreichend restriktiv geregelt ist und einem System effektiver Kontrolle unterliegt. Damit kann die Weite der Speicherungspflicht nicht durch andere Faktoren kompensiert werden.