

Anna Höning (geb. Michel)

Externe Rechtskontrolle der Nachrichtendienste

Band 7

Anna Höning (geb. Michel)

Externe Rechtskontrolle
der Nachrichtendienste

digital | recht
Staat und digitale Gesellschaft

Herausgegeben von
Prof. Dr. Matthias Bäcker, LL.M.
Prof. Dr. Roland Broemel
Prof. Dr. Thomas Burri, LL.M.
Prof. Dr. Albert Ingold
Prof. Dr. Antje von Ungern-Sternberg
Prof. Dr. Silja Vöneky

Trier, 2024

Band 7

Anna Höning, geboren 1994; Wissenschaftliche Mitarbeiterin am Lehrstuhl für Öffentliches Recht und Informationsrecht, Datenschutzrecht der Johannes Gutenberg-Universität Mainz von 2021 bis 2024.

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dieses Buch steht gleichzeitig als elektronische Version über den Publikations- und Archivierungsserver OPUS der Universität Trier <https://ubt.opus.hbz-nrw.de/home> und über die Webseite der Schriftenreihe <https://digitalrecht-oe.uni-trier.de> zur Verfügung.

Dieses Werk ist unter der Creative-Commons-Lizenz vom Typ CC BY 4.0 International (Namensnennung) lizenziert: <https://creativecommons.org/licenses/by/4.0/>

Von dieser Lizenz ausgenommen sind Abbildungen, an denen keine Rechte der Autorin/des Autors oder der UB Trier bestehen. Covergestaltung von Monika Molin.



ISBN: 9783759865076

URN: urn:nbn:de:hbz:385-20241021115000225-1554329-9

DOI: <https://doi.org/10.25353/ubtr-1022-4737-1023>

© 2024 Anna Höning

Mainz

Die Schriftenreihe wird gefördert von der Universität Trier und dem Institut für Recht und Digitalisierung Trier (IRDT).

Anschrift der Herausgeber: Universitätsring 15, 54296 Trier

Vorwort

Die vorliegende Arbeit wurde im Herbst 2024 am Fachbereich Rechtswissenschaften der Johannes Gutenberg-Universität Mainz als Dissertation angenommen. Der Stand der Bearbeitung ist August 2024.

Mein Dank gilt zunächst Professor Dr. Matthias Bäcker, der für seine Doktoranden immer ansprechbar ist, von dem ich sehr viel lernen durfte und der mich ausgezeichnet betreut hat. Hätte er mich und andere Studierende im Januar 2020 nicht eingeladen, ihn zur Mündlichen Verhandlung am Bundesverfassungsgericht zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes zu begleiten, wäre mein Interesse am Sicherheitsrecht vielleicht nie geweckt worden.

Für die sehr zügige Erstellung des Zweitgutachtens bedanke ich mich herzlich bei Professor Dr. Albert Ingold und für die Übernahme des Vorsitzes bei Professor Dr. Mathias Cornils. Ferner danke ich dem Herausgeberkreis der Schriftenreihe digital|recht für die Aufnahme als Autorin.

All den Mitarbeitern, die in den Landtagen und Behörden meine Anfragen beantwortet haben, danke ich herzlich.

Auch Jun.-Prof. Dr. Sebastian Golla und Dr. Johannes Marosi möchte ich danken, ohne ihre Ermutigung hätte ich das Projekt Dissertation nicht begonnen.

Dr. Rebecca John und Dr. Theresa Busch möchte ich dafür danken, dass sie viele Pausen bereichert haben und mir stets mit Rat und Tat zur Seite standen.

Herzlichen bedanken möchte ich mich auch bei Ulrike Naumann, Ralph Igel und Dr. Konstantin von Notz, mit denen ich oft über das Nachrichtendienstrecht nachgedacht habe und von denen ich viel lernen durfte.

Der größte Dank gilt jedoch meiner Familie, vor allem meinem Ehemann und meiner Mutter, allen voran aber meinem Vater, der seitdem ich schreiben kann mein Korrektor und Diskussionspartner ist: dabei hat er von der Fabel in der Grundschule bis zu einem sehr langen Text über Nachrichtendienstkontrolle ein breites Interessenspektrum und außerordentliches Durchhaltevermögen bewiesen. Danke, Papa.

Mainz, August 2024

Anna Höning

Inhaltsübersicht

Inhaltsverzeichnis

Einleitung

Teil 1

Von der Kontrolle und den Kontrollierten.....5

Teil 2

Vorgaben für die externe Rechtskontrolle nach höherrangigem Recht.....63

Teil 3

Vereinbarkeit des einfachen Rechts mit höherrangigen Vorgaben..... 223

Teil 4

Reformvorschlag für die externe Rechtskontrolle der Nachrichtendienste..... 317

Teil 5

Thesen..... 383

Inhaltsverzeichnis

Vorwort.....	I
Inhaltsübersicht	III
Inhaltsverzeichnis	V
Abkürzungsverzeichnis	XXIII
<i>Einleitung</i>	1
<i>Teil 1</i>	5
Von der Kontrolle und den Kontrollierten	5
A. Definition der externen Rechtskontrolle.....	5
I. Begriff der Externen Rechtskontrolle	5
1. Kontrolle.....	5
a. Definition von Kontrolle	5
b. Abgrenzung zur Aufsicht	6
2. Rechtskontrolle.....	8
3. Externe Rechtskontrolle	10
4. Ausgeklammerter Bereich.....	10
II. Funktionsbestandteile von Kontrolle	12
1. Kontrolleur	12
2. Kontrollmittel	12
3. Kontrollierter und Kontrollgegenstand.....	13
4. Kontrollmaßstab	13
5. Kontrollnorm	13
6. Verhaltensnormen	14
7. Kontrollergebnis	14
8. Kontrollverhältnis	14
9. Anwendung auf diese Untersuchung	15
III. Maßstäbe für die Analyse und Bewertung von Kontrolle	15

1. Initiative	15
2. Zeitpunkt	16
3. Modalität	16
4. Distanz.....	17
5. Kontrollmittel zur Informationsgewinnung.....	17
6. Kontrollerggebnisfolgen.....	18
7. Fachkompetenz	19
8. Kontrolltiefe	19
9. Klare Kontrollstrukturen	19
10. Kontrollniveau	19
11. Barrieren	20
12. Effektivität und Effizienz	21
13. Kontrollexzesse	22
B. Nachrichtendienste als Kontrollierte.....	22
I. Staatsrechtliche Verortung.....	22
1. Verfassungsschutz des Bundes	23
2. Landesverfassungsschutz.....	24
3. Militärischer Abschirmdienst	25
4. Bundesnachrichtendienst	25
II. Gesetzliche Aufträge.....	26
1. Gemeinsamkeiten	26
a. Politische Information	26
b. Gefahrenfrüherkennung	27
aa) Bundesnachrichtendienst.....	27
bb) Bundesamt für Verfassungsschutz und Militärischer Abschirmdienst....	27
2. Zusammenarbeit mit Gefahrenabwehr- und Strafverfolgungsbehörden.....	29
a. Klassische Abgrenzung	29
b. Trennungsgebot und informationelles Trennungsprinzip.....	29
c. Annäherung der Tätigkeiten und verstärkte Kooperation	31
3. Auftrag der Verfassungsschutzbehörden	33
a. Bundesamt für Verfassungsschutz	34

aa) Eigene Aufgaben	34
(1) § 3 Abs. 1 BVerfSchG	34
(2) § 3 Abs. 1 Nr. 2, 3, 4 BVerfSchG BVerfSchG	35
(3) Bestrebungen	35
(4) Tatsächliche Anhaltspunkte	36
(5) Aufklärung der Gesellschaft.....	36
bb) Problemfall organisierte Kriminalität	36
cc) Mitwirkungspflichten	38
b. Landesämter für Verfassungsschutz	39
aa) Organisierte Kriminalität.....	39
bb) Fortwirkende Strukturen der Deutschen Demokratischen Republik (DDR).....	40
cc) Öffentlichkeitsaufklärung und Prävention	40
4. Auftrag des Militärischen Abschirmdienstes	42
5. Auftrag des Bundesnachrichtendienstes.....	42
III. Befugnisse	43
1. Überblick über die Art der Befugnisse.....	43
a. Generalklausel zur Informationserhebung	44
b. Telekommunikationsüberwachung	45
c. Quellen-Telekommunikationsüberwachung	45
d. Online-Durchsuchung	46
e. Strategische Fernmeldeaufklärung.....	46
f. Eingriffe in informationstechnische Systeme von Ausländern im Ausland	47
g. Observationen	48
h. Verdeckte Mitarbeiter und Vertrauensleute	48
i. Verdeckte Ton- und Bildaufzeichnungen (außerhalb oder innerhalb der Wohnung)	49
j. Auskunftsverlangen gegenüber Privatunternehmen	50
k. Verdeckte Erhebung von Daten aus Sozialen Medien	53
l. IMSI/IMEI Catcher	53
m. Sonstige Befugnisse	54
n. Auswertung und Übermittlung.....	54
2. Keine abschließende Normierung.....	54
3. Tatbestandliche Weite der Befugnisnormen	55
a. Beispiele für weite Regelungen	56
b. Vorgaben aus der Entscheidung zum Bayerischen Verfassungsschutzgesetz..	57
c. Gründe für die tatbestandliche Weite.....	58
4. Schlüsselfaktor für die Kontrolltiefe	59
IV. Intransparenz der Verarbeitung	61

<i>Teil 2</i>	63
Vorgaben für die externe Rechtskontrolle nach höherrangigem Recht	63
A. Verfassungsrechtliche Determinanten der externen Rechtskontrolle	63
I. Kontrollbedürfnis	63
1. Demokratieprinzip	64
2. Rechtsstaatsprinzip	65
3. Kompensationsthese	66
a. Kompensation der heimlichen Vorgehensweise	66
b. Kompensation gelockerter materieller Bindungen	66
4. Steigerung der Kontrollbedürftigkeit	67
5. Fazit	68
II. Einschlägige Grundrechte	68
III. Vorgaben des Bundesverfassungsgerichts	71
1. Duales Kontrollkonzept des BVerfG: Richterliche bzw. richterähnliche Vorabkontrolle und nachträgliche Datenschutzkontrolle	71
a. Grundsatz	72
aa) Kontrollmaßstab	72
bb) Zeitpunkt	72
cc) Kontrolleur	73
dd) Distanz	74
ee) Modalitäten	74
ff) Initiative	75
gg) Kontrollmittel zur Informationsgewinnung	76
hh) Kontrollerggebnisfolgen	77
ii) Fachkompetenz und Ressourcen	79
jj) Kontrollgegenstand- und tiefe	79
kk) Kontrollniveau	80
ll) Barrieren	81
b. Sonderfall strategische Ausland-Fernmeldeüberwachung	82

aa) Kontrollmaßstab	82
bb) Zeitpunkt.....	82
cc) Kontrolleur.....	83
dd) Distanz.....	84
ee) Modalitäten	84
ff) Initiative	84
gg) Kontrollmittel zur Informationsgewinnung	85
hh) Kontrollergebnisfolgen.....	85
ii) Fachkompetenz und Ressourcen	86
jj) Kontrollgegenstand- und tiefe	87
kk) Kontrollniveau	87
ll) Barrieren.....	88
mm) Fazit	88
2. Zweistufiges Kernbereichskonzept	89
a. Grundsatz.....	90
b. Einbindung einer unabhängigen Stelle.....	90
aa) Kontrollmaßstab	91
bb) Flexible Vorgabe bei Telekommunikationsüberwachung und dem Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten	91
3. Verfassungsrechtliche Herleitung der Kontrollmodi	92
a. Art. 10 GG	92
aa) Tatbestandsvoraussetzungen	92
(1) Schutzgüter	92
(2) „Dienen“	93
bb) Rechtsfolge: Nachprüfung.....	95
cc) Auslegung des Bundesverfassungsgerichts	96
(1) Erstes Abhörurteil.....	96
(2) Zweite Abhörentscheidung.....	98
(3) Drittes Abhörurteil	98
dd) Frühere Sonderstellung von Art. 10 GG	99
ee) Kein ausschließliches Kontrollmandat der G 10-Kommission	100
b. Art. 13 GG.....	102
c. Art. 1 Abs. 1 GG.....	102
d. Verhältnismäßigkeitsgrundsatz	103
aa) Vorabkontrolle.....	103
bb) Datenschutzkontrollen.....	103
cc) Eingriffsintensität als entscheidender Faktor	105
4. Eingriffsintensität nachrichtendienstlicher Mittel.....	105
a. Faktoren zur Festlegung der Eingriffsintensität im Sicherheitsrecht.....	106

aa) Art der Daten	106
bb) Anlass für die Informationserhebung	108
cc) Umstände der Erhebung	109
dd) Betroffener Personenkreis	110
ee) Denkbare Verwendung	110
b. Typisierte Bestimmung der Eingriffsintensität	111
aa) Besonders schwere Grundrechtseingriffe	112
(1) Wohnraumüberwachung und Online-Durchsuchung	112
(2) Eingriffe in informationstechnische Systeme von Ausländern im Ausland	113
(3) Strategische Überwachung	114
bb) Schwere Grundrechtseingriffe	115
(1) (Quellen-)Telekommunikationsüberwachung	115
(2) Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern	115
(3) Längerfristige Observation	117
(4) Ton- und Bildaufzeichnungen außerhalb von Wohnungen	117
(5) Auskunftsverlangen gegenüber Privatunternehmen über Kontobewegungen und Verkehrsdaten	118
(6) IMSI/IMEI-Catcher	118
cc) Mittelschwere Grundrechtseingriffe	119
(1) Einsatz von Vertrauensleuten und Verdeckten Ermittlern	119
(2) Sonstige Auskunftsverlangen gegenüber Privatunternehmen	119
(3) Datenerhebung aus Social Media	120
(4) Kurzfristige Observationen	120
dd) Leichte Grundrechtseingriffe	121
ee) Fazit	121
ff) Abweichende Bewertung bei Maßnahmen des MAD?	121
(1) Abstrakte Kenntnis der Überwachungsmöglichkeit und Verfassungstreuepflicht	122
(2) Auswirkungen auf die Kriterien	123
(3) Höhere Eingriffsintensität	124
5. Kontroll- Gesamtüberblick	124
a. Realität der additiven Anwendung nachrichtendienstlicher Mittel	125
b. Additiver Grundrechtseingriff	125
c. Kontroll-Gesamtüberblick	126
aa) Maßnahmen einer Behörde	127
bb) Nicht jede Maßnahme	127
d. Zwischenergebnis	127

6. Gleichwertigkeit bzw. Gerichtsähnlichkeit der Vorabkontrolle	127
a. Konkretisierung des Bundesverfassungsgerichts	128
b. Grenzen weitergehender Vorgaben	129
aa) Weitergehende Anforderungen in der Literatur	129
bb) Grenzen	129
(1) Unterscheidung zwischen richterlicher und gerichtsähnlicher Kontrolle	129
(2) Regelungsspielraum des Gesetzgebers	131
(3) Zwischenergebnis	131
7. Fazit der Rechtsprechungsanforderungen	131
IV. Kritische Würdigung der Rechtsprechung	132
1. Entwicklung der Diskussion	132
a. Notstandsverfassung, Einführung des G 10 und Abhörentscheidungen	133
b. Schaffung der Datenschutzbeauftragten und Meilenstein Volkszählungsurteil	136
c. Konflikt zwischen dem BfDI und der G 10-Kommission	137
d. Enthüllungen von Edward Snowden	139
e. Schaffung des Unabhängigen Gremiums	140
f. Entscheidung zur strategischen Ausland-Fernmeldeaufklärung	141
g. Entscheidung zum Bayerischen Verfassungsschutzgesetz	142
2. Kritikwürdige Aspekte	143
a. Fokussierung auf Vorabkontrollen	143
aa) Hervorgehobene Bedeutung der Vorabkontrolle	143
bb) Vorteile und Erwartungen	145
cc) Zweifel an der Kompensation der Heimlichkeit durch Vorabkontrollen	146
dd) Zweifel an der Kompensation weiterer Befugnisse	147
(1) Abmilderung des rechtsstaatlichen Defizits statt Kompensation	148
(2) Widersprechender Praxisbericht	149
ee) Fokussierung teilweise ungerechtfertigt	149
b. Vernachlässigung der Datenschutzkontrolle	150
aa) Vorteile der laufenden Kontrolle	150
bb) Kontrollergebnisfolgen	150
cc) Kontrollintervall	151
c. Quasi-gesetzgeberische Rolle des Vorabkontrolleurs	152
d. Schaffung eines (zu) mächtigen Akteurs?	153

aa) Minderheitenrechte	153
bb) Veröffentlichung von Entscheidungsgründen	154
cc) Rechtfertigungsdruck gegenüber dem Parlamentarischen Kontrollgremium	154
dd) Fazit.....	155
e. Nebeneinander von Kontrollstrukturen.....	155
f. Zu detaillierte Ableitung aus der Verhältnismäßigkeit.....	156
g. Richtervorbehalt als effektivstes Mittel?.....	159
aa) Institutionelle Neutralität	159
bb) Fehlende Sensibilität für Grundrechtsschutz durch Verfahren	159
cc) Umfang	160
dd) Geheimhaltungsbedenken.....	161
ee) Vorwurf der mangelnden Kompetenz.....	162
ff) Zwischenergebnis	163
B. Völkerrechtliche und unionsrechtliche Vorgaben an die Kontrollnormen	163
I. Völkerrechtliche Maßgaben: die Europäische Menschenrechtskonvention	164
1. Innerstaatliche Wirkung.....	164
2. Einschlägiges Konventionsrecht	165
3. Extraterritoriale Wirkung der EMRK	166
4. Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte.....	168
a. Standards für gezielte, personenbezogene Maßnahmen	170
aa) Ex ante-Genehmigung.....	172
bb) Kontrolle während der Durchführung der Maßnahme	174
cc) Ex post-Kontrolle.....	176
dd) Drei Stufen-Kontrolle: Leitbild oder zwingende Vorgabe?	177
b. Vorgaben für die Kontrolle von „Massenüberwachung“	177
aa) Begriff der „bulk interception“	178
bb) Vier Stufen der Strategischen Überwachung	179
cc) „Ende zu Ende-Schutzmechanismen“	179
dd) Ex ante-Genehmigung.....	179
ee) Kontrolle während der Durchführung.....	181
ff) Ex post-Kontrolle	183
gg) Verbindlichkeit der Vorgaben	184
c. Relevanz der Eingriffsintensität	186
aa) Eindeutige Relevanz für die Kontrolle der Massenüberwachung	186
bb) Geringere Bedeutung für gezielte Überwachung.....	187
II. Unionsrechtliche Vorgaben.....	189

1. Anwendungsbereich des Unionsrechts: Ausnahme zur „nationalen Sicherheit“	189
a. Definition der „nationalen Sicherheit“ in der Literatur	190
b. Definition der „nationalen Sicherheit“ durch den EuGH	191
aa) Schutzobjekt	192
bb) Art der staatlichen Reaktion	193
cc) Drohende Schäden	193
(1) Art der Schäden	193
(2) „Unmittelbar“	193
(3) Beispiel der „terroristischen Aktivitäten“	195
c. Tätigkeiten der Nachrichtendienste im Anwendungsbereich des Unionsrechts	196
aa) Spezifische Eigenschaften der staatlichen Reaktion zur Abgrenzung erforderlich?	196
bb) Schutzobjekt	197
cc) Art der staatlichen Reaktion	197
dd) Drohende Schäden	197
(1) Weit gefasster Auftrag des BND	197
(2) Allgemeine Bekämpfung der organisierten Kriminalität	198
(3) „Unmittelbare“ Bedrohung bei jeglicher Vorfeldaufklärung?	199
(4) Öffentlichkeitsarbeit und Prävention als Reaktion bei „unmittelbarer“ Bedrohung?	200
ee) Zwischenergebnis	200
d. Negative Auswirkung der Definition	201
e. Aktuellere Definition des EuGH?	202
2. Einschlägiges Sekundärrecht: DSGVO oder JIRL?	203
a. Anwendbarkeit der JIRL	204
aa) Auslegung von Art. 1 Abs. 1 JIRL	204
bb) Subsumtion der nachrichtendienstlichen Aufträge	205
cc) Vorgaben der JIRL	209
(1) Befugnisse der Aufsichtsbehörde, Art. 47 JIRL	209
(2) Sonstige Regelungen	211
b. Anwendbarkeit der DSGVO	212
aa) Allgemeine Gefahrenabwehr	212
bb) Übermittlung von Privaten an die Nachrichtendienste	212
cc) Vorgaben der DSGVO	214
3. Unionsgrundrechte	215
a. Anwendbarkeit	215
b. Materielle Vorgaben zur Kontrolle der Nachrichtendienste	216

aa) Vorratsdatenspeicherung	216
bb) Schrems II.....	217
(1) Gegenstand der Entscheidung	217
(2) Eingriffe in Artt. 7, 8 GRCh.....	217
(3) Eingriffe in Art. 47 GRCh	219
(4) Verallgemeinerbare Aussagen?.....	220
cc) Art. 52 Abs. 3 GRCh i. V. m. Art. 8 EMRK	221
4. Fazit: Mindestens teilweise Anwendbarkeit des Unionsrechts	221
<i>Teil 3</i>	223
Vereinbarkeit des einfachen Rechts mit höherrangigen Vorgaben	223
A. Vorabkontrollen bei eingriffsintensiven Maßnahmen.....	223
I. Vorabkontrollen de lege lata.....	223
1. Richtervorbehalt.....	224
a. Wohnraumüberwachung	224
b. Sonstige Befugnisse	224
2. Genehmigungsvorbehalte zugunsten der G 10-Kommission	225
a. Auskunftersuchen	225
b. Ton- und Bildaufzeichnungen außerhalb von Wohnungen	227
c. IMSI/IMEI-Catcher	227
d. Funkzellenabfrage.....	228
e. Längerfristige Observationen	228
f. Einsatz von Vertrauensleuten und Verdeckten Ermittlern	228
g. Quellen-Telekommunikationsüberwachung.....	229
h. Online-Durchsuchung	229
3. Genehmigungsvorbehalt zugunsten des Unabhängigen Kontrollrats des Bundes	229
II. Änderungsbedarf.....	230
1. Langfristige Observationen	230
2. Einsatz von Vertrauensleuten und Verdeckten Ermittlern	230
3. IMSI/IMEI-Catcher	231
B. Rechtskontrolle der G 10-Kommissionen	231
I. Kontrollmaßstab	232
II. Kontrollgegenstand und -tiefe	232
1. Vorabkontrolle.....	232
a. Grundsatz	232
b. Ausnahme: Eilfall.....	233

2. Entscheidung über die Benachrichtigung Betroffener	234
3. Datenschutzkontrolle	235
III. Zeitpunkt	236
IV. Kontrolleur	236
1. Anzahl der (stellvertretenden) Mitglieder	236
2. Ernennung der G 10-Kommission	238
a. Wahl der Mitglieder	238
b. Anbindung an die Legislative	238
c. Möglichkeit zur erneuten Wahl	240
3. Stellung als Parlamentarier und Ehrenamtlichkeit	241
a. Tätigkeit als Abgeordnete	241
b. Ehrenamtlichkeit der Mitglieder	242
4. Mehrheitsfindung innerhalb der Kommissionen	243
5. Geheimhaltung	243
V. Distanz	244
VI. Modalitäten	245
1. Differenzierung nach der Aufgabe	245
2. Sitzungsrhythmus	245
a. Bundesebene	245
b. Länderebene	246
VII. Initiative	246
VIII. Kontrollmittel zur Informationsgewinnung	247
1. Unterrichtungspflicht	247
2. Auskunfts-, Einsichts- und Zutrittsrecht	247
a. Umfang	247
b. Anspruchsberechtigte	248
c. Einschränkungen der Rechte	249
IX. Kontrollerggebnisfolgen	249
X. Fachkompetenz und Ressourcen	250
1. Fachkompetenz	250
2. Ressourcen	251
a. „Notwendige“ Personal- und Sachausstattung	251
b. Geschäftsstellen	251
c. Mitarbeiter mit technischem Sachverstand	253
d. Rechte der Mitarbeiter	253
e. Einbindung des Bundes- oder Landesdatenschutzbeauftragten	253
f. Beauftragung des Ständigen Bevollmächtigten	254
XI. Kontrollniveau	254
XII. Barrieren	254

1. Ressourcenbarrieren	254
2. Third Party Rule-Einwand	255
a. Begründung für die Notwendigkeit	255
b. Missbrauchsgefahr	256
c. Unzulässig gegenüber unabhängigen Instanzen der Rechtskontrolle	256
C. Rechtskontrolle des Unabhängigen Kontrollrats	257
I. Kontrollmaßstab	257
II. Kontrollgegenstand	258
1. Gerichtsähnliches Kontrollorgan	258
a. Vorabkontrolle des GeKon	258
aa) Strategische Ausland- Fernmeldeüberwachung gem. § 19 BNDG	259
(1) Reichweite der Kontrolle	259
(2) Verletzung von Konventionsrecht	260
bb) Gezielte Erhebungen gem. §§ 20, 21 Abs. 2 BNDG	261
(1) Reichweite der Kontrolle	261
(2) Verfassungswidrige Ausklammerung der Kontrolle von Suchbegriffen	262
(3) Verfassungswidrige Ausnahme von der Vorabkontrolle	262
cc) Feststellung des „qualifizierten Aufklärungsbedarfs“ bei Kooperationen	262
dd) Möglicher Kernbereichsbezug von Daten aus der strategischen Ausland- Fernmeldeaufklärung und der Online-Durchsuchung von Ausländern im Ausland	263
ee) Eingriffe in informationstechnische Systeme gem. § 34 BNDG	263
ff) Übermittlung von Daten aus Vertraulichkeitsbeziehungen	264
b. Sonstige Rechtmäßigkeitskontrolle „nach dem Vollzug“	265
2. Administratives Kontrollorgan	266
a. Zuständigkeit	267
b. Notwendigkeit eines Positivkatalogs?	268
c. Verfassungswidrigkeit wegen fehlender Protokollierungspflicht	268
III. Zeitpunkt	269
IV. Kontrolleur	269
1. Gerichtsähnliches Kontrollorgan	270
a. Anzahl der Mitglieder, Ernennung, Amtszeit und Organisation	270
b. Rekrutierung der Mitglieder aus obersten Bundesrichtern	270
c. Stellung als Beamte	271
d. Mehrheitsfindung	271
e. Geheimhaltung	271
f. Verfahren	272

2. Administratives Kontrollorgan	272
a. Besetzung	273
b. Verfahren.....	273
V. Distanz.....	273
VI. Modalitäten	275
VII. Initiative	276
VIII. Kontrollmittel zur Informationsgewinnung	276
1. Kontrollmittel	276
2. Verfassungsrechtliche Bedenken	277
a. Gesteigerte Anforderung für die Einsichtnahme in Originale.....	277
b. Ausnahme vom Zutrittsrecht bei „Ausnahmesituationen“	277
c. Kein Schutz gegen Falschaussagen	278
d. Keine Zwangsbefugnisse zur Durchsetzung von § 56 BNDG	278
IX. Kontrollerggebnisfolgen	279
1. Gerichtsähnliches Kontrollorgan	279
2. Administratives Kontrollorgan	279
3. Bericht an das Parlamentarische Kontrollgremium und den Bundestag.....	280
X. Fachkompetenz und Ressourcen.....	281
XI. Kontrollniveau	282
XII. Barrieren	283
D. Rechtskontrolle der Datenschutzbeauftragten.....	284
I. Folge der generellen Verneinung des Anwendungsbereichs von Unionsrecht	284
II. Datenschutzkontrolle des Einsatzes nachrichtendienstlicher Mittel.....	284
1. Maßstab der Kontrolle und Rechtsgrundlagen	285
a. Rechtsgrundlage auf der Bundesebene	285
b. Rechtsgrundlagen auf der Landesebene	285
c. Rechtmäßigkeitskontrolle als wesentlicher Bestandteil der Datenschutzkontrolle	286
d. Spezielle Einbindung der Datenschutzbeauftragten.....	287
2. Unproblematische rechtskonforme Aspekte.....	288
a. Kontrolleur	288
b. Zeitpunkt.....	288
c. Distanz	288
d. Initiative.....	288
3. Modalität	289
4. Ressourcen	290
a. Stellenanteile	290

aa) Bund	290
bb) Länder.....	291
b. Ressourcenmangel in den Ländern	292
5. Kontrollmittel zur Informationsgewinnung.....	293
a. Unterstützungspflicht.....	293
b. Akteneinsichts- und Auskunftsrecht.....	293
c. Zutrittsrecht	294
d. Beauftragung von Mitarbeitern	294
e. Keine vergleichbaren Kontrollmittel in Mecklenburg-Vorpommern	294
f. Weitreichende Ausnahmetatbestände.....	295
6. Kontrollerggebnisfolgen.....	295
a. Kontrollerggebnisfolgen de lege lata	295
b. Grundsätzliche Option der Erwähnung im Tätigkeitsbericht.....	297
c. Beanstandung als wirksame Befugnis?	297
d. Teilweise Unionsrechtswidrigkeit.....	299
7. Barrieren	299
a. Unzureichende personelle Ressourcen	299
b. Rechtliche Kontrollhindernisse.....	299
aa) Ausnahmetatbestände	300
(1) Unwirksamkeit der Befugnisse	301
(2) Lösungsmöglichkeiten	302
bb) Zuständigkeitsvorbehalt zugunsten der G 10-Kommission.....	303
III. Parallele Zuständigkeit bei der strategischen Ausland-Fernmeldeüberwachung und bei Eingriffen in informationstechnische Systeme von Ausländern im Ausland.....	304
E. Die Kernbereichsschutzkonzepte	305
I. Ausgestaltung der (unabhängigen) Stelle	305
1. Keine Stelle	305
2. Keine unabhängige Stelle.....	306
3. Unabhängige Stellen	307
II. Reichweite der Einbindung.....	307
III. Art der Einbindung.....	308
1. Wohnraumüberwachung und Online-Durchsuchung.....	308
2. Strategische Ausland-Fernmeldeüberwachung und Eingriffe in informationstechnische Systeme von Ausländern im Ausland	310
F. Kontroll-Gesamtüberblick	311
I. Kontroll-Gesamtüberblick de lege lata	312

1. Zuständigkeitsvorbehalt zugunsten der G 10-Kommission	313
2. Kooperationsnorm.....	313
II. Zwischenergebnis	313
G. Fazit: Defizite der einfach-rechtlichen Ausgestaltung	314
<i>Teil 4</i>	317
Reformvorschlag für die externe Rechtskontrolle der Nachrichtendienste.....	317
A. Reformbedarf	317
I. Vielzahl der Kontrolleure.....	317
II. Aufwand für die Kontrollierten	319
III. Hohe Komplexität	320
IV. Mangel an Ressourcen	320
V. Staatswohl- Einrede	321
B. Eckpunkte für einen Reformvorschlag.....	321
I. Reform der externen Rechtskontrolle auf der Bundesebene	321
1. Vereinfachtes Kontrolldesign	322
a. Zentralisierung der Vorabkontrolle beim GeKon	322
b. Datenschutzkontrolle durch den BfDI und Auflösung des AdKon	323
aa) Zuständigkeit des BfDI für sonstige Datenschutzkontrollen der Nachrichtendienste	323
bb) Vermeidung von Interessenskonflikten bei Kontrolle des AdKon.....	324
cc) Kontroll-Gesamtüberblick	325
dd) Keine unbehebbar Nachteile.....	325
(1) Third Party Rule-Einwand	325
(2) Höheres Rechtsschutzniveau	326
(3) Lähmung der Datenschutzaufsicht	326
(4) Verzahnung mit GeKon	327
ee) Abgrenzung zum GeKon	327
(1) Teilzuständigkeit des GeKon für die Datenschutzkontrolle.....	328
(2) Abstimmungsbedarf	329
c. Auflösung der G 10-Kommission	329
2. GeKon als „unabhängige Stelle“ zum Kernbereichsschutz	330
3. Rechtsgrundlagen für die Kontrolle durch das GeKon.....	330
a. Kontrollgegenstand des gerichtsähnlichen Kontrollorgans	331

aa) Kontrolle der strategischen Ausland-Fernmeldeüberwachung	331
bb) Vorabkontrolle von Vereinbarungen mit ausländischen Partnerdiensten	331
cc) Ausweitung auf alle eingriffsintensiven nachrichtendienstlichen Befugnisse	332
dd) Vorabkontrolle in Eilfällen.....	333
b. Kontrolleur	333
aa) Betroffenenvertreter	333
(1) Vor- und Nachteile.....	334
(2) Ausgestaltung	335
bb) Eingabemöglichkeit an das PKGr	336
(1) Grund.....	336
(2) Mögliche Einwände.....	336
(3) Enge Ausgestaltung	338
cc) Öffnung des Bewerberkreises.....	338
dd) Auswahlmöglichkeit des Parlamentarischen Kontrollgremiums.....	340
c. Distanz	340
d. Initiative	340
aa) Beschwerderecht der Betroffenen	340
bb) Direkter digitaler Zugriff.....	343
e. Kontrollmittel zur Informationsgewinnung	343
aa) Umfassende Protokollierung der Verarbeitungsschritte	343
bb) Beschwerdemöglichkeit für Whistleblower aus den Nachrichtendiensten	343
cc) Anordnung	344
(1) Begründungstiefe.....	344
(2) Sanktionsbefugnis gegenüber dem BND.....	345
dd) Kontrollmittel für einzelne Mitglieder des GeKon.....	345
ee) Durchsetzungsinstrumente	345
(1) Durchsetzung der Kontrollmittel und Schutz gegen Falschaussagen	346
(2) Durchsetzung gegenüber dem Nachrichtendienst und der Aufsichtsbehörde	346
f. Kontrollerggebnisfolgen	348

aa) Genehmigungsentscheidung	348
(1) Begründungspflicht für Entscheidungen	348
(2) Veröffentlichung von Entscheidungsgründen	349
(3) Möglichkeit zu Sondervoten	349
bb) Austausch mit dem Parlamentarischen Kontrollgremium	350
(1) Separate Norm zur Kooperation mit dem UKRat	351
(2) Berichterstattung gegenüber dem Parlamentarischen Kontrollgremium	351
g. Fachkompetenz und Ressourcen	352
4. Datenschutzkontrolle durch den BfDI	353
a. Kontrollgegenstand	353
b. Modalität	353
c. Initiative	355
d. Stärkung der Kontrollmittel des BfDI	355
e. Stärkung der Kontrollergebnisfolgen des BfDI	356
aa) Anordnungsbefugnis	356
bb) Einzelfallberichterstattung gegenüber dem PKGr	357
f) Abbau von Barrieren	357
aa) Rechtliche Kontrollbarrieren	358
bb) Ressourcenbarrieren	359
5. Umsetzung des Kontrollgesamtüberblicks	359
a. Umfassendes Einsichtsrecht des BfDI	359
b. Verstärkte Kooperation zwischen den Aufsichtsbehörden	359
6. Der BfDI als internationaler Ansprechpartner	360
7. Evaluierung von Kontrolllücken	361
8. Zwischenergebnis	361
II. Reform der externen Rechtskontrolle auf der Landesebene	362
1. Auflösung der G 10-Kommissionen	362
2. Vorabkontrolle durch ein Landes-GeKon?	363
3. Vorabkontrolle durch Richter	364
a. Vorteile der gerichtlichen Vorabkontrolle auf der Landesebene	365
b. Neuregelung des Bayerischen Verfassungsschutzgesetzes	366

aa) Befugnisse mit Richtervorbehalt	366
(1) Verdeckte Mitarbeiter (Art. 18 BayVSG)	366
(2) Vertrauensleute (Art. 19 BayVSG)	367
(3) Längerfristige Observationen (Art. 19a BayVSG)	367
(4) Komplexe qualifizierende Anforderungen für den Richtervorbehalt	368
bb) Ausgestaltung der richterlichen Kontrolle	370
cc) Kernbereichsschutzvorkehrungen	371
dd) Beibehaltung der G 10-Kommission	371
c. Neuregelung des Hessischen Verfassungsschutzgesetzes	372
aa) Befugnisse mit Richtervorbehalt	372
(1) Einsatz von IMSI-Catchern zur Ermittlung eines Standorts (§ 9 Abs. 1 HVSG)	372
(2) Längerfristige Observationen (§ 11 Abs. 2, 4 HVSG)	373
(3) Verdeckte Mitarbeiterinnen und Mitarbeiter (§ 12 HVSG)	373
(4) Vertrauensleute (§ 13 HVSG)	374
bb) Ausgestaltung der richterlichen Kontrolle	374
(1) § 5 a HVSG	374
(2) Sonderregelung für die Vorabkontrolle des Einsatzes von Verdeckten Mitarbeitern und Vertrauensleuten	374
(3) Keine Abschirmung des Gerichts	376
cc) Kernbereichsschutzvorkehrungen	376
dd) Beibehaltung der G 10-Kommission	376
d. Faktoren für die gesetzliche Ausgestaltung	376
aa) Zuständiges Gericht	377
bb) Ressourcen	377
cc) Räumliche Abschirmung des Gerichts	377
dd) Personelle Abschirmung: Sicherheitsüberprüfung der Richter	377
(1) Richterliche Unabhängigkeit gem. Art. 97 GG	378
(2) § 2 Abs. 3 Nr. 2 SÜG	379
4. Auflösung der Doppelzuständigkeit mit G 10-Kommission	380
5. Richter als „unabhängige Stellen“ für den Kernbereichsschutz	381
6. Datenschutzkontrollen durch die Landesdatenschutzbeauftragten	381
7. Kontroll-Gesamtüberblick	382
III. Fazit	382
<i>Teil 5</i>	383
Thesen	383
Literaturverzeichnis	393

Abkürzungsverzeichnis

AdKon	Administratives Kontrollorgan des Unabhängigen Kontrollrats
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BVerfSchG	Bundesverfassungsschutzgesetz
BA	Bundeskriminalamt
BKAG	Bundeskriminalamtsgesetz
BND	Bundesnachrichtendienst
BNDG	Bundesnachrichtendienstgesetz
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EUV	Vertrag über die Europäische Union
FISC	Foreign Intelligence Surveillance Court
GeKon	Gerichtsähnliches Kontrollorgan des Unabhängigen Kontrollrats
HUMINT	Human Intelligence: die Erhebung nachrichtendienstlich relevanter Erkenntnisse durch menschliche Quellen
JIRL	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den Militärischen Abschirmdienst
PKGr	Parlamentarisches Kontrollgremium des Bundes
PKGrG	Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes
RaIS	Recht auf informationelle Selbstbestimmung
RaViIS	Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme
UKRat	Unabhängiger Kontrollrat

Einleitung

„[T]he secret world and accountability are not mutually incompatible.“

Venedig Kommission, 2015¹

Die Bundesrepublik Deutschland zählt insgesamt 19 Nachrichtendienste². Neben einem Auslandsnachrichtendienst, dem Bundesnachrichtendienst, und einem auf die Bundeswehr spezialisierten Nachrichtendienst, dem Militärischen Abschirmdienst, existieren 16 Inlandsnachrichtendienste, denn jedes Bundesland betreibt ein Landesamt für Verfassungsschutz. Diese werden ergänzt durch eine Behörde auf Bundesebene, das Bundesamt für Verfassungsschutz (Teil 1). Alle Nachrichtendienste haben gemein, dass ihre Tätigkeit der externen Rechtskontrolle unterworfen ist. Für die externe Rechtskontrolle zuständig sind nach geltendem Recht die G 10-Kommissionen, der Unabhängige Kontrollrat, der Bundesdatenschutzbeauftragte, die Landesdatenschutzbeauftragten sowie die Gerichte.

Diese externe Rechtskontrolle der Nachrichtendienste näher zu beleuchten, ist das Anliegen der Untersuchung. Aber was ist unter dem Begriff der „externen Rechtskontrolle“ zu verstehen? Rechtskontrolle ist eine Form der Kontrolle, bei der der Maßstab, an dem man den Vergleich ausrichtet, die Rechtmäßigkeit ist.³ Mit dem Adjektiv „extern“ werden die betrachteten Kontrollorgane von der Rechtsaufsicht abgegrenzt, die durch dieselbe oder eine übergeordnete Behörde erfolgt.

Das Nachrichtendienstrecht ist ein noch junges Rechtsgebiet, das „sich als eine überaus zerfaserte, auf zahlreiche Gesetze verteilte Materie“ darstellt, „welche einer inneren Ordnung weitgehend entbehrt“. ⁴ Diese zu analysieren und zu ordnen, hat sich die Wissenschaft in den letzten Jahren mehr und mehr zur Aufgabe gemacht. Neben

¹ Venedig-Kommission, Report 2015, S. 58 Rn. 272.

² Das Militärische Nachrichtenwesen wird mangels einer gesetzlichen Regelung und Beschreibung seines Aufgabenbereichs sowie seiner Befugnisse aus der Bearbeitung ausgeklammert.

³ Vgl. im Detail [Teil 1](#); Backer, Hdb. des Verfassungsrechts, 1715, 1754; Kahl, Kontrolle, 459, 481; zum Mastab der Rechtmaigkeit: Kempny, Verwaltungskontrolle, S. 20.

⁴ Loffelmann/Zoller, Nachrichtendienstrecht, S. 5.

umfangreichen Sammelwerken zum Nachrichtendienstrecht⁵ wurden zahlreiche Monografien⁶ veröffentlicht, darunter spezifisch solche zur Rechtskontrolle der Nachrichtendienste⁷. Worin also besteht der Mehrwert dieser Untersuchung?

Erstens werden die Vorgaben des Bundesverfassungsgerichts zur externen Rechtskontrolle der Nachrichtendienste analysiert. Das ist nötig, weil die Rechtsprechung in jüngster Zeit erheblich weiterentwickelt wurde.⁸

Zweitens wird die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu nachrichtendienstlichen Befugnissen in die Betrachtung miteinbezogen.⁹ Die sich aus der Judikatur des EGMR ergebenden Vorgaben zur Kontrolle der Nachrichtendienste bleiben im nationalen Fachrecht teilweise unberücksichtigt, mit der Folge, dass diese Normen konventionswidrig sind.

Drittens wird analysiert, ob und inwieweit der Anwendungsbereich des Unionsrechts eröffnet ist, wenn es um die Tätigkeit der Nachrichtendienste geht. Die herrschende Meinung ist überzeugt, dass der Anwendungsbereich des Unionsrechts nicht eröffnet sei, weil die „nationale Sicherheit“ gem. Art. 4 Abs. 2 S. 3 EUV Sache der Mitgliedstaaten ist. Die neueste Rechtsprechung des EuGH und dessen Definition der „nationalen Sicherheit“ zwingen jedoch dazu, diese Gewissheit in Frage zu stellen.

Viertens wird das Landesrecht miteinbezogen, denn bisher existiert lediglich eine Ausarbeitung, in der die Rechtskontrolle einer Landesverfassungsschutzbehörde untersucht wird.¹⁰ Das wird der Bedeutung der Landesämter für Verfassungsschutz jedoch nicht gerecht. In der Praxis haben die Landesverfassungsschutzbehörden eine gegenüber dem BfV nicht zu vernachlässigende Relevanz. Das zeigt schon ein Blick auf ihre personelle Ausstattung. Denn obwohl die einzelnen Verfassungsschutzbehörden der Länder weitaus weniger Mitarbeiter beschäftigen als das BfV, verfügen sie in ihrer Gesamtheit über vergleichbare Ressourcen: Während das Bundesamt im Jahr 2022 4.286 Mitarbeiter beschäftigte, arbeiteten für die Landesverfassungsschutzbehörden insgesamt circa 3.600 Personen, Tendenz steigend. Gerade auf der Landesebene ist der Reformbedarf wegen einzelner verfassungs- und konventionswidriger Normen hoch.

⁵Unter anderem *Dietrich/Eiffler* (Hrsg.), Hdb. des Rechts der Nachrichtendienste; *Schenke/Graulich/Ruthig* (Hrsg.) Sicherheitsrecht des Bundes, *Dietrich et al.* (Hrsg.), Hdb. Sicherheits- und Staatschutzrecht.

⁶Unter anderem *Vogt*, Strategische Auslandsstelekkommunikationsüberwachung; *Knaust*, Matrix einer neuen Generation auslandsnachrichtendienstlicher Überwachungstätigkeit; *Winter*, Kohärenz des Nachrichtendienstrechts; *Banzhaf*, Präventionsbehörden.

⁷*Alt*, Kompensatorische Kontrolle; *Bantlin*, G 10-Kommission; *Kornblum*, Rechtsschutz; *Gusy*, Grundrechte und Verfassungsschutz.

⁸2024 ist die erste ausführliche Darstellung veröffentlicht worden: *Alt*, Kompensatorische Kontrolle.

⁹Zur strategischen Ausland-Fernmeldeaufklärung bereits *Knaust*, Matrix einer neuen Generation auslandsnachrichtendienstlicher Überwachungstätigkeit.

¹⁰*Gusy*, der die Kontrolle durch die G 10-Kommission in NRW ausführlich analysiert, *Gusy*, Grundrechte und Verfassungsschutz, S. 15 ff.

Viele gravierende verfassungswidrige Aspekte wurden bisher auch im Laufe mehrerer Reformen nicht behoben, was die Notwendigkeit unterstreicht, dass die Analyse des Landesrechts aus rechtsstaatlicher Perspektive nicht vernachlässigt werden darf.

Fünftens wurde ein breiter Ansatz gewählt, der sowohl die G 10-Kommissionen als auch den UKRat und die Kontrolle durch die Datenschutzbeauftragten berücksichtigt. Der Vorteil dieses Ansatzes ist, dass ein Gesamtüberblick zur externen Rechtskontrolle entsteht.

Alle fünf Aspekte sind bisher als solche kaum untersucht, insbesondere jedoch in ihrer Wechselwirkung nicht analysiert worden.

Nach der Entscheidung des Bundesverfassungsgerichts zum Bayerischen Verfassungsschutzgesetz vom April 2022 steht das Nachrichtendienstrecht vor umfassenden Reformen. Dabei sollte insbesondere auf der Länderebene die Chance ergriffen werden, eine vollumfänglich verfassungs- und konventionskonforme Rechtslage zu schaffen. Wenn die Untersuchung dem Gesetzgeber und der Praxis dabei eine (weitere) nützliche Quelle sein kann, hat sie ihren Zweck bereits erreicht.

Die nach der aktuellen Rechtsprechung des Bundesverfassungsgerichts zwingende Reform des Nachrichtendienstrechts findet zu einem Zeitpunkt statt, in dem sich die sicherheitspolitische Lage in Europa wegen des Angriffskriegs Russlands auf die Ukraine deutlich verschlechtert hat. Mit den sicherheitspolitischen Herausforderungen ist auch die Bedeutung der Nachrichtendienste gestiegen.¹¹ Rechtsstaatlichkeit als Richtschnur ist dabei „kein Hindernis“, denn wir „können es uns schlicht nicht leisten, die Nachrichtendienste aufgrund verfassungswidriger Befugnisse oder mittels unregulierter oder unkontrollierter Praktiken tätig werden zu lassen, weil wir damit gerade das beschädigen würden, was zu schützen ihre und unsere Aufgabe ist – und weil wir damit eben jenen Extremisten argumentativ in die Hände spielen, welche die Lauterkeit und Wehrhaftigkeit unserer Demokratie bewusst in Frage stellen“.¹²

Wir sollten uns vor dem Hintergrund der angespannten sicherheitspolitischen Lage aber auch nicht erlauben, unklare Kontrollarchitekturen bestehen zu lassen und den Nachrichtendiensten auf diese Weise ineffizienten Mehraufwand zuzumuten. Die Regelungsvorschläge in diesem Text beruhen auf der Annahme, dass Kontrollstrukturen – entgegen weit verbreiteter Überzeugungen¹³ – bei entsprechender gesetzlicher Ausgestaltung kein Hindernis für die nachrichtendienstliche Arbeit darstellen.

¹¹ Vgl. u.a. <https://www.handelsblatt.com/politik/deutschland/bnd-und-verfassungsschutz-nicht-ausreichend-leistungsfähig-ampelpolitiker-wollen-geheimdienste-staerken/28919434.html> (abgerufen am 31.8.2024).

¹² Rede des Vorsitzenden des Parlamentarischen Kontrollgremiums in der 20. Wahlperiode, Dr. Konstantin von Notz (MdB), beim 4. Symposium zum Recht der Nachrichtendienste am 30.6.2022, *Notz, Extremismusbekämpfung*, 113, 118.

¹³ So zum Beispiel BND Präsidenten a.D. *Schindler/Hanning*, Gastbeitrag: „Diese ausufernde Kontrollbürokratie ist die Schwester der Ineffizienz.“

Zu Beginn dieser Untersuchung wird ausgeführt, was unter „externe Rechtskontrolle“ zu verstehen ist und wie die Tätigkeit der Nachrichtendienste geregelt ist (Teil 1). Der Schwerpunkt der Untersuchung liegt in der Beantwortung der Frage, welche Vorgaben des Verfassungsrechts, der Europäischen Menschenrechtskonvention und des Unionsrechts bei der Ausgestaltung der externen Rechtskontrolle der Nachrichtendienste zu beachten sind (Teil 2). Sodann wird analysiert, inwieweit diese Vorgaben auf der einfach-rechtlichen Ebene, in den Fachgesetzen auf der Bundes- und Länderebene, berücksichtigt werden (Teil 3). Die Untersuchung schließt mit einem Eckpunkte-Vorschlag zur Reform der externen Rechtskontrolle, der (unter Wahrung der höherrangigen Vorgaben) eine Lösung für häufig kritisierte Probleme des jetzigen Kontrolldesigns anbietet (Teil 4). Für einen schnellen Zugriff auf die Ergebnisse wird auf das Thesenkapitel verwiesen (Teil 5).

Teil 1

Von der Kontrolle und den Kontrollierten

A. Definition der externen Rechtskontrolle

Um die Rechtskontrolle der Nachrichtendienste zu untersuchen, bietet es sich zunächst an, den verwaltungswissenschaftlichen Kenntnisstand über „Kontrolle“ zu rezipieren. Auf diese Weise sollen der Begriff der „externen Rechtskontrolle“ präzisiert (I.) und die notwendigen oder möglichen Bestandteile einer Rechtskontrolle identifiziert werden (II.). Die Analyse der Rechtskontrolle der Nachrichtendienste setzt gedankliche Ankerpunkte voraus, anhand derer man die Kontrolle untersuchen und bewerten kann. Deshalb ist die Frage zu beantworten, welche – für diese Arbeit sinnvoll einsetzbaren – Maßstäbe die Verwaltungsrechtswissenschaft zur Analyse von Kontrollmechanismen entwickelt hat (III.).

I. Begriff der Externen Rechtskontrolle

Der Begriff der externen Rechtskontrolle setzt sich aus mehreren Elementen zusammen, die zunächst abzugrenzen sind: Was ist unter Kontrolle (1.), was unter Rechtskontrolle (2.) und was unter externer Rechtskontrolle (3.) zu verstehen? Bestimmte Bereiche werden aus der Betrachtung bewusst ausgeklammert (4.).

1. Kontrolle

Zunächst ist zu klären, wie „Kontrolle“ hier ausgelegt und von der „Aufsicht“ abgegrenzt wird.

a. Definition von Kontrolle

Für die Frage, wie „Kontrolle“ im verwaltungsrechtswissenschaftlichen Sinn definiert werden sollte, existiert bisher keine allgemeingültige Antwort.

Weit verbreitet ist eine Definition, wonach Kontrolle der Vergleich von einem Istwert mit einem Sollwert ist.¹ Dabei entspricht der Istwert² der „Realität“ und der Sollwert dem jeweils angelegten „Richtmaß“; das Ziel des Vergleichs besteht darin, entweder die Übereinstimmung oder die Abweichung der beiden Werte zu erkennen.³ Dabei muss beachtet werden, dass dieser Vergleich nur *annähernd* objektiv sein kann, da er durch menschliche Bewertungen statt durch exakte – ggf. maschinelle – Messungen erfolgt.⁴

Über diesen Vergleich hinaus muss der Kontrollbegriff sich auf die Möglichkeit zur steuernden Einflussnahme erstrecken, sodass der Kontrolleur den Kontrollierten in Richtung des angestrebten Sollwertes korrigieren bzw. zum Tätigwerden veranlassen kann.⁵ Diese Einwirkung durch die Kontrolleure ist grundsätzlich nicht als ständige „Mitwirkung“ gedacht, sondern als aus der Distanz die möglichen Probleme antizipierendes, nur im Fall des Versagens handelndes „Sicherheitsnetz“.⁶ Richtigerweise muss Kontrolle so weit verstanden werden, dass davon Vorabkontrollen erfasst werden, deren Ziel es ist, Missbrauch von vornherein zu verhindern, sodass nicht erst dann reagiert werden kann, „wenn das Kind bereits in den Brunnen gefallen ist“.⁷

b. Abgrenzung zur Aufsicht

Die Begriffe „Kontrolle“ und „Aufsicht“⁸ werden häufig identisch verwendet.⁹ Dennoch existieren Ansätze, mit denen die Begriffe voneinander abgegrenzt werden können. Sie sollen knapp¹⁰ rezipiert werden, um zu erklären, wieso für die Zwecke dieser

¹ *Krebs*, Kontrolle, S. 17; *Kempny*, Verwaltungskontrolle, S. 16; *Schmidt-Aßmann*, Verwaltungskontrolle, 9, 10; *Hahn*, Aufsicht, S. 38; *Bantlin*, G 10-Kommission, S.88; *Eiffler*, Hdb. des Rechts der Nachrichtendienste, 1499, 1503 Rn.5.

² Bantlin weist überzeugend darauf hin, dass der „Ist-Wert“ bei der Nachrichtendienstkontrolle aufgrund der Heimlichkeit nachrichtendienstlicher Tätigkeit nicht offensichtlich sei, *Bantlin*, G 10-Kommission, S. 92.

³ *Kabl*, Kontrolle, 459, 461 Rn. 4.

⁴ Daraus folgt eine erhöhte Bedeutung der Kompetenz für und Legitimation von Kontrolle, *Krebs*, Kontrolle, S. 17.

⁵ Dieses „Element der Berichtigung“ als „mittlerweile herrschende Meinung“ deklarierend: *Kabl*, Kontrolle, 459 Rn. 5 f.; vgl. auch *Guber*, DVBl 2019, 902, 903; *Arnim*, Kontrolle, 1316; *Krebs*, Kontrolle, S. 44; *Hansalek*, Parlamentarische Kontrolle, S. 149; *Scheuner*, Verantwortung und Kontrolle, 379, 390. Manche Autoren warnen sogar (hinsichtlich der Parlamentarischen Kontrolle) vor einem „Wächter ohne Schwert“, vgl. z.B. *Gusy*, ZRP 2008, 36, 39.

⁶ *Hoffmann-Riem*, Verwaltungskontrolle, 325, 353.

⁷ *Arnim*, DöV 1982, 917.

⁸ Gemeint ist nur die Kontrolle der Verwaltung, nicht die Aufsicht über Private, *Schmidt-Aßmann*, Verwaltungskontrolle, 9, 13.

⁹ U.a. *Arnim*, Kontrolle, 1316, 1317; *Hahn*, Aufsicht, S. 37; die Begriffe synonym verwendend auch *Brunner*, Kontrolle, S. 164.

¹⁰ Vertiefend *Kabl*, Kontrolle, 459, 466 f.

Arbeit der Begriff der Kontrolle, nicht der der Aufsicht verwendet wird.

Ein Differenzierungsansatz stellt darauf ab, dass bei der Kontrolle die Möglichkeit zur Einwirkung auf den Kontrollierten zwar bestehen könne, anders als bei der Aufsicht aber die Kompetenz zur Berichtigung nicht zwingend sei.¹¹ Wenn man (wie hier) davon ausgeht, dass Kontrolle ebenfalls ein sanktionierendes Element enthält, taugt dieser Ansatz zur Abgrenzung nicht.

Eine weitere Überlegung geht dahin, dass die Aufsicht oft (aber nicht zwingend) innerhalb eines hierarchischen Verhältnisses erfolge, während Kontrolle meistens (aber nicht zwingend) durch eine Koordination und Kooperation von Kontrolleur und Kontrolliertem geprägt sei.¹² Die in der Untersuchung betrachteten Kontrolleure – der UKRat, die Datenschutzbeauftragten sowie die G 10-Kommissionen – stehen zu den Nachrichtendiensten in keinem Über- oder Unterordnungsverhältnis. Anders zu beurteilen ist dies beispielsweise bei den übergeordneten Ministerien, den Aufsichtsbehörden, in deren Weisungsstrang die Nachrichtendienste eingegliedert und denen sie somit nachgeordnet sind. Mangels eines Über-/Unterordnungsverhältnisses zwischen den hier betrachteten Institutionen und den Nachrichtendiensten wäre „Kontrolle“ nach diesem Ansatz die richtige Bezeichnung. Gegen diese Überlegung zur Abgrenzung spricht, dass auch Kontrolle hierarchische Elemente enthalten kann, wenn beispielsweise der Kontrolleur Sanktionen verhängt, während Aufsicht andererseits kooperative Elemente haben kann; eine trennscharfe Differenzierung ermöglicht auch dieser Ansatz daher nicht.¹³

Außerdem wird der Grundsatz der Gewaltenteilung zur Differenzierung herangezogen: Demnach sei die Staatsaufsicht innerhalb einer staatlichen Gewalt verortet, die Kontrolle hingegen erfolge durch eine andere Gewalt oder Dritte, wie beispielsweise die Öffentlichkeit.¹⁴

Während der BfDI wie die Nachrichtendienste Teil der Exekutive ist, handelt es sich bei den G 10-Kommissionen und dem UKRat um Staatsorgane „sui generis“, die sich keiner der drei Staatsgewalten eindeutig zuordnen lassen¹⁵. Der UKRat ist zwar wie der

¹¹ *Hahn*, Aufsicht, S. 38; *Kabl*, Kontrolle, 459, 466.

¹² *Kabl*, Kontrolle, 459, 466 f.; *Hahn*, Aufsicht, S. 37 f.; auch *Scheuner*, Verantwortung und Kontrolle, 379, 390.

¹³ *Kabl*, Kontrolle, 459, 467 Rn. 17.

¹⁴ *Kabl*, Kontrolle, 459, 466 f.; *Schmidt-Aßmann*, Verwaltungskontrolle, 9, 13 f.; *Bantlin*, G 10-Kommission, S. 91.

¹⁵ *Barczak*, KritV 2021, 91, 128, a. A. Tombrink, der den UKRat „schwerpunktmäßig“ der rechtsprechenden Gewalt zuordnet, *Tombrink*, GSZ 2024, 28, 32; zum Vorgänger des UKRat, dem Unabhängigen Gremium: *Schenke/Graulich/Ruthig/Dietrich*, § 16 BNDG Rn.3; zur G 10-Kommission: *BVerfG*, Beschluss vom 20.6.1984 - 1 BvR 1494/78 - Rn. 40; *Schenke/Graulich/Ruthig/Huber*, § 15 G 10 Rn. 13 ff.

BfDI eine unabhängige, oberste Bundesbehörde und somit formal Teil der Exekutive¹⁶. Da er wie die G 10-Kommissionen funktional jedoch gerichtsähnliche Aufgaben wahrnimmt¹⁷, ist er ebenfalls als Staatsorgan „sui generis“ einzuordnen.¹⁸

Nach diesem Ansatz müsste man die Tätigkeit des BfDI als Aufsicht bezeichnen, die der anderen Institutionen hingegen als Kontrolle. Da es sich bei der Kontrolle um den Oberbegriff handelt, der die Aufsicht als speziellere Kontrollart miteinschließt¹⁹, ist die Anwendung des Kontrollbegriffs auf die Tätigkeit des BfDI jedenfalls nicht falsch.

Nach den beiden letztgenannten Differenzierungsansätzen liegt es im Ergebnis näher, von Kontrolle zu sprechen, weshalb dieser Begriff gewählt wurde.

2. Rechtskontrolle

Die Rechtskontrolle ist eine Form der Kontrolle, bei der der Maßstab, an dem man den Vergleich ausrichtet, die Rechtmäßigkeit ist.²⁰

Die Kontrolle durch die hier in den Fokus gerückten Kontrolleure wird stattdessen teilweise nach den Gewalten strukturiert, denen die kontrollierende Einheit angehört: So wird nach justiziellen, exekutiven und parlamentarischen Kontrollen unterschieden.²¹ Durch diese Begrifflichkeiten wird allerdings der Maßstab der Kontrolle offengelassen. Demgegenüber stellt der Begriff der Rechtskontrolle auf den Vorgang der Kontrolle ab (hier: Überprüfung der Rechtmäßigkeit; bei der politischen Kontrolle: (zusätzlich) Bewertung politischer Aspekte) und trifft keine Aussage über die Gewaltenzugehörigkeit der kontrollierenden Einheit, was für diese Untersuchung von Vorteil ist, weil sich die Kontrollorgane nicht derselben Gewalt zuordnen lassen.

Das Ziel der Rechtskontrolle ist es, ausschließlich die Rechtmäßigkeit des Verwaltungshandelns zu prüfen. Darin liegt der wesentliche Unterschied zur politischen Kontrolle²², die zwar Rechtmäßigkeitsprüfungen zum Gegenstand haben kann, deren Zweck aber anders gelagert ist: Die Organe politischer Kontrolle beabsichtigen, nachträglich die Behördenpraxis zu erfassen, die Rechtslage zu evaluieren, politische Veränderungen anzustoßen, Missstände aufzudecken und politische Verantwortlichkeiten

¹⁶ BT-Drs.19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 100; *Schmidt-Räntsch*, K&R 2022, 34, 37.

¹⁷ *Barczak*, KritV 2021, 91, 128.

¹⁸ So im Ergebnis auch *Alt*, Kompensatorische Kontrolle, S. 156, 161.

¹⁹ M. w. N. *Kahl*, Kontrolle, 459, 466.

²⁰ *Bäcker*, Hdb. des Verfassungsrechts, 1715, 1754; *Kahl*, Kontrolle, 459, 481; zum Maßstab der Rechtmäßigkeit: *Kempny*, Verwaltungskontrolle, S. 20.

²¹ Vgl. z.B. *Eiffler*, Hdb. des Rechts der Nachrichtendienste, 1499, 1503 Rn. 5; *Bantlin*, G 10-Kommission, S. 105 f.

²² Der Begriff wird synonym zum Begriff der „parlamentarischen Kontrolle“ verwendet.

herzustellen.²³ Politische Kontrolle stellt – im Gegensatz zur Rechtskontrolle – explizit (auch) die Frage nach der Zweckmäßigkeit.²⁴

Die politische Kontrolle der Nachrichtendienste ist in die Fachaufsicht durch die zuständigen Ministerien²⁵, die allgemeine parlamentarische Kontrolle durch die Abgeordneten und die institutionalisierte Kontrolle durch dafür eingerichtete, parlamentarische Kontrollgremien (Parlamentarisches Kontrollgremium, Vertrauensgremium gem. § 10a Abs. 2 BHO, Gremium gem. Art. 13 Abs. 6 S. 2 GG) gegliedert. Dass ein spezielles parlamentarisches Kontrollgremium auf Bundesebene eingerichtet werden muss, ist über Art. 45d GG verfassungsrechtlich abgesichert. Auf der Länderebene existieren teilweise vergleichbare Verfassungsnormen. Unabhängig davon sind die speziellen Kontrollgremien bundesweit einfach-rechtlich vorgesehen.²⁶ Zur Aufklärung von (vermuteten) Missständen in den Nachrichtendiensten werden außerdem vermehrt Untersuchungsausschüsse eingesetzt.²⁷

Die politische Kontrolle und die Rechtskontrolle sind „grundsätzlich verschieden“, weshalb die eine gegen die andere nicht „aufgerechnet“ werden kann.²⁸

²³ Kornblum, Rechtsschutz, S. 80; Bäcker, Hdb. des Verfassungsrechts, 1715, 1755; „politische Erfolgskontrolle“ genannt bei Schmidt-Aßmann, Verwaltungskontrolle, 9, 20; Bezeichnung als „umfassende Kontrolle“ bei Hirsch, Kontrolle, S. 103, 116; Schneider, Fernmeldegeheimnis, S. 286; hinzu kommt, dass die politischen Kontrolleure weitere Aufgaben haben: „The body may be full or part-time, but even if it is parttime, the supervision exerted is likely to be more continuous than that exercised by a parliamentary body, the members of which have many other political interests and responsibilities“, Venedig-Kommission, Report 2015, S. 50 Rn. 229; zudem gibt es Anhaltspunkte dafür, dass die Rechtskontrolle durch die politischen Kontrollorgane wegen politischer Interessen in der Praxis problematisch sein kann, Bull, DöV 2008, 751, 753.

²⁴ Singer, § 1 Rn. 31; vgl. beispielhaft im Abschlussbericht des 1. NSU-Untersuchungsausschusses, BT-Drs. 17/14600 v. 22.8.2013, S. 854 ff.; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 300: „(...) Ausdruck der allgemeinen parlamentarischen Verantwortung für die sachgerechte und politisch angemessene Aufgabenwahrnehmung der Exekutive“.

²⁵ Für die Kontrolle der Nachrichtendienste ist die Fachaufsicht wegen ihrer Nähe zu den Nachrichtendiensten von enormer Bedeutung, vgl. insoweit Gärditz, EuGRZ 2018, 6, 17.

²⁶ Die Normen unterscheiden sich teilweise erheblich voneinander, vgl. Michel, GSZ 2021, 197 f.

²⁷ Auf Bundesebene beispielsweise der NSA-Untersuchungsausschuss, NSU-Untersuchungsausschuss 1 und 2.

²⁸ Zur politischen Kontrolle durch das Parlament: „Insoweit kann auch die eine nicht gegen die andere Kontrolle aufgerechnet werden. In der Diktion traditioneller Staatsrechtswissenschaft gesprochen: Demokratie und Rechtsstaat haben unterschiedliche normative Gehalte und Funktionsmodi, welche zumindest partiell unterschiedliche Verwirklichungs- und Durchsetzungsmechanismen und -instanzen erfordern.“, Gusy, Grundrechte und Verfassungsschutz, S. 129; vgl. insoweit zu generellen Nachteilen der parlamentarischen Kontrolle, Venedig-Kommission, Report 2007, Rn. 151.

3. Externe Rechtskontrolle

Das Adjektiv „extern“ dient der Abgrenzung der in die Untersuchung einbezogenen Kontrolleure von der internen Rechtskontrolle, die durch dieselbe oder eine übergeordnete Behörde erfolgt.²⁹ Ein Beispiel für einen behördeninternen Aufsichtsmechanismus ist der Behördenleitervorbehalt. So müssen bestimmte nachrichtendienstliche Tätigkeiten teilweise vom Behördenleiter genehmigt werden³⁰, was mit einer (erneuten) Prüfung der rechtlichen Voraussetzungen verbunden ist. Gem. § 2 Abs. 4 ThürVerfSchG gibt es im thüringischen Verfassungsschutz eine „Stabsstelle Controlling“, die die Recht- und Zweckmäßigkeit von Handlungen der Fachabteilungen hausintern kontrolliert. Darüber hinaus prüfen die übergeordneten Ministerien im Rahmen der Fachaufsicht unter anderem die Rechtmäßigkeit der nachrichtendienstlichen Tätigkeit.³¹

Im Gegensatz dazu handelt es sich bei den G 10-Kommissionen, dem UKRat und den Datenschutzbeauftragten um externe Kontrolleure, weil sie weder Teil der Nachrichtendienste noch ihnen übergeordnet sind.

4. Ausgeklammerter Bereich

Neben der internen Rechtskontrolle wird auch die nachträgliche gerichtliche Kontrolle ausgeklammert. Das dürfte Verwunderung hervorrufen, weil die in der Rechtsordnung praktisch bedeutendste Form der (Rechts-)Kontrolle diejenige durch die Gerichte ist³². Die Entscheidung, die nachträgliche gerichtliche Kontrolle nicht näher zu beleuchten, ist in ihrer Andersartigkeit zur Kontrolle durch die G 10-Kommissionen, den UKRat und die Datenschutzbeauftragten begründet: Anders als die Kontrolle durch diese Kontrolleure ist die nachträgliche gerichtliche Kontrolle der Gerichte auf einen Betroffenen angewiesen, der die Kontrolle anstößt, indem er Klage erhebt. Denn die gerichtliche Kontrolle basiert auf der Grundentscheidung zum Individualrechtsschutz³³: Auf die Initiative des Einzelnen hin entscheiden die Verwaltungsgerichte einen Einzelfall (Art. 19 Abs. 4 GG, §§ 42 Abs. 2, 113 VwGO). Diese Individualbezogenheit des gerichtlichen Rechtsschutzsystems verengt zwangsläufig den Umfang der Kontrolle: Wenn Klagebefugte davon absehen, ihr Recht durchzusetzen oder ihnen der Nachweis nicht gelingt, findet keine Kontrolle statt.³⁴

²⁹ Bantlin/Graulich, GSZ 2023, 179, 182.

³⁰ Beispielsweise in § 9a Abs. 2 S. 5, § 15 Abs. 2 S. 2 BVerfSchG; § 11 Abs. 6 S. 5 HVSG.

³¹ Eißler, Hdb. des Rechts der Nachrichtendienste, 1499, 1506 Rn. 9 f.

³² Schmidt-Aßmann, Verwaltungskontrolle, 9, 21; Bantlin, G 10-Kommission, S. 96.

³³ Schmidt-Aßmann, Ordnungsidee, S. 22; Wöckel, Hdb. des Rechts der Nachrichtendienste, 1607 Rn. 1a; Bantlin, G 10-Kommission, S. 90; Kahl, Kontrolle, 459, 527.

³⁴ Schmidt-Aßmann, Verwaltungskontrolle, 9, 22.

Die grundsätzliche Kritik am gerichtlichen Rechtsschutz potenziert sich, wenn die handelnde Verwaltungsbehörde ein Nachrichtendienst ist.³⁵ Weil die Tätigkeiten der Nachrichtendienste überwiegend geheim sind und sie den Betroffenen deshalb verborgen bleiben³⁶, fordert das Bundesverfassungsgericht mit Verweis auf Art. 19 Abs. 4 GG, dass Betroffene nachträglich über den Einsatz von eingriffsintensiven nachrichtendienstlichen Mitteln informiert werden müssen.³⁷ Die Rechtsgrundlagen normieren – unter Billigung durch das BVerfG – Ausnahmen von der grundsätzlichen Informationspflicht.³⁸ Wer infolge einer Ausnahmeregelung von dem Einsatz nachrichtendienstlicher Mittel nichts weiß, wird keine Klage erheben, was die Häufigkeit von gerichtlichen Kontrollen erheblich einschränkt.³⁹ Hinzu kommt, dass der gerichtliche Rechtsschutz auf Antrag des Betroffenen notwendigerweise auf die nachträgliche Kontrolle beschränkt ist. Eine nachträgliche Überprüfung kann Grundrechtseingriffe durch ungerechtfertigte Informationserhebung jedoch nicht ungeschehen machen.⁴⁰

Demgegenüber hat die externe Rechtskontrolle durch den UKRat, die G 10-Kommissionen und die Datenschutzbeauftragten den Vorteil, dass sie als objektive, von der Geltendmachung einer Verletzung subjektiver Rechte unabhängige Rechtskontrolle ausgestaltet ist. Hierin liegt ihre Stärke gegenüber der einzelfallbezogenen gerichtlichen Rechtskontrolle im Recht der Nachrichtendienste, denn die Initiative liegt nicht alleine⁴¹ beim Betroffenen. Zudem kontrollieren der UKRat, die G 10-Kommissionen und die Datenschutzbeauftragten unabhängig von der Kenntnis des Betroffenen und damit auch ohne dessen Einbindung. Ihre Kontrollen sollen gerade den weitgehenden, strukturell bedingten Wegfall der gerichtlichen Kontrolle im Nachrichtendienstrecht ausgleichen.⁴² Die Kontrollen haben aber nicht zwingend Individualmaßnahmen zum

³⁵ Grundlegend zur gerichtlichen Kontrolle: *Kornblum*, Rechtsschutz.

³⁶ *Wöckel*, Hdb. des Rechts der Nachrichtendienste, 1607 Rn. 1b; *Hirsch*, Kontrolle, S. 61 f., 120 f.; *Gusy*, *VerwArch* 2015, 437, 440; *Bull*, *DöV* 2008, 751.

³⁷ Zur Benachrichtigungspflicht aus Art. 19 Abs. 4 GG bei heimlichen Grundrechtseingriffen: st. Rspr. BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 179; BVerfG, Urteil v. 3.3.2004 - 1 BvR 2378/98 - Rn. 292; BVerfG, Beschluss v. 13.6.2007 - 1 BvR 1550/03 - 1 BvR 2357/04 - 1 BvR 603/05 Rn. 170; *Kornblum*, Rechtsschutz, S. 233; *Wöckel*, Hdb. des Rechts der Nachrichtendienste, 1607, 1623 Rn. 17.

³⁸ Mit Art. 19 Abs. 4 GG sind diese Einschränkungen unter bestimmten Voraussetzungen vereinbar, vgl. BVerfG - Urteil v. 14.7.1999 - 1 BvR 2420/95 Rn. 197, 287 ff.; einfach-gesetzlich normiert z.B. in § 15 Abs. 2 BVerfSchG; § 12 Abs. 1 G 10. *Bantlin* weist unter Bezugnahme auf die Berichte des PKGr darauf hin, dass Mitteilungen in der Praxis eher die Ausnahme darstellen, *Bantlin*, G 10-Kommission, S. 106.

³⁹ *Kornblum*, Rechtsschutz, S. 117; die Rechtsschutzgarantie als faktisch leerlaufend bezeichnend: *Gusy*, *VerwArch* 2015, 437, 440; vgl. [Teil 1 B.IV](#).

⁴⁰ Dazu *Bantlin*, G 10-Kommission, S. 97. Es bleibt allerdings die Möglichkeit, zukünftige Grundrechtseingriffe zu verhindern.

⁴¹ Trotzdem können Betroffene Kontrollen anstoßen, vgl. u. a. § 15 Abs. 5 S. 1 Var. 2 G 10, § 28 Abs. 1 BVerfSchG.

⁴² BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 273; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

Gegenstand, so prüft der BfDI beispielsweise häufig die Rechtmäßigkeit ganzer Verarbeitungsprogramme, die eine Vielzahl von Personen betreffen⁴³.

Die Losgelöstheit vom Betroffenen und die fehlende Beschränkung auf Individualmaßnahmen sprechen dafür, die Rechtskontrolle durch die genannten Organe separat zu untersuchen und dabei den gerichtlichen Rechtsschutz auszuklammern.

II. Funktionsbestandteile von Kontrolle

Um die skizzierte externe Rechtskontrolle der Nachrichtendienste analysieren zu können, wird das von *Kempny* entwickelte „Untersuchungs- und Beschreibungswerkzeug“⁴⁴ angewandt.⁴⁵ Der Kontrollvorgang wird auf diese Weise in seine Bestandteile aufgegliedert und näher beschrieben.

1. Kontrolleur

Der Kontrolleur ist nach *Kempny* diejenige Einheit, der das bewertende menschliche Verhalten zugerechnet wird. Im Rahmen dieses Untersuchungsgegenstands sind das de lege lata die G 10-Kommissionen, der BfDI, die Landesdatenschutzbeauftragten sowie der UKRat.

2. Kontrollmittel

Die Befugnisse, die dem Kontrolleur verliehen werden, damit er seine Kontrolle ausüben kann, werden Kontrollmittel genannt. Welche Kontrollmittel den Rechtskontrollleuren der Nachrichtendienste rechtlich zur Verfügung stehen, wird in dieser Untersuchung analysiert.

⁴³ Vgl. 30. Tätigkeitsbericht des BfDI, 2021, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/30TB_21.pdf?__blob=publicationFile&cv=13 (zuletzt abgerufen am: 31.8.2024), S. 85.

⁴⁴ *Kempny*, Verwaltungskontrolle, S. 3, 4.

⁴⁵ Soweit nicht anders gekennzeichnet, gilt für diesen Abschnitt, dass für die Anwendung seines Modells *Kempny* selbst zitiert wurde, *Kempny*, Verwaltungskontrolle, S. 18 - 26.

3. Kontrollierter und Kontrollgegenstand

Kontrollierter ist diejenige Einheit, der das bewertete menschliche Verhalten zugerechnet wird. Das Verhalten selbst wird als Kontrollgegenstand betitelt. Bei mehreren organisatorischen Ebenen soll nach *Kempny* eine Zurechnung an alle Ebenen erfolgen⁴⁶, diese Zurechnung könne jedoch je nach Zuschnitt der Untersuchung begrenzt werden.

Kontrollierte sind die Nachrichtendienste, das heißt der BND, das BfV und die sechzehn Verfassungsschutzbehörden sowie der Militärische Abschirmdienst. Der BND ist dem Bundeskanzleramt nachgeordnet, der MAD dem Bundesverteidigungsministerium und die Verfassungsschutzbehörden dem jeweiligen Innenministerium (vgl. § 1 Abs. 1 BNDG, § 1 Abs. 1 MADG, § 2 Abs. 1 BVerfSchG).

Der Kontrollgegenstand ist die nachrichtendienstliche Tätigkeit.⁴⁷ Im Rahmen dieser Tätigkeit wenden die Mitarbeiter der Nachrichtendienste die ihnen verliehenen Befugnisse zur Erfüllung ihres nachrichtendienstlichen Auftrags an.⁴⁸ Der Kontrollgegenstand kann auf bestimmte nachrichtendienstliche Tätigkeiten begrenzt sein.

4. Kontrollmaßstab

Der Kontrollmaßstab ist nach diesem Modell eine anzugebende Eigenschaft, die ein (nach Urheber und Zeit eindeutig bestimmtes) menschliches Verhalten entweder aufweist oder nicht. Ein solcher Maßstab kann nach *Kempny* unter anderem die Rechtmäßigkeit sein. Ein Verhalten sei rechtmäßig, wenn es im Einklang mit allen geltenden Ge- oder Verboten sei; rechtswidrig, wenn es sie verletze. Mit der Begrenzung der Dissertation auf die Rechtskontrolle ist die Entscheidung für diesen Kontrollmaßstab getroffen.

5. Kontrollnorm

Kontrollnormen sind in *Kempnys* Modell alle Normen, die an den Kontrolleur adressiert sind und dessen Verhalten bestimmen. Sie berechtigen oder verpflichten zur Kontrolle und enthalten den Kontrollmaßstab. Die höherrangigen Vorgaben für Kontrollnormen zu erklären und die einfach-rechtliche Ausgestaltung derselben zu analysieren, ist ein Ziel dieser Untersuchung (vgl. Teil 2).

⁴⁶ Die Zurechnung könne sich nach *Kempny* sogar auf die gesamte Staatsgewalt erstrecken. Unter anderem, weil die Kontrolleure teilweise selbst der Exekutive angehören, wird darauf für diese Untersuchung verzichtet.

⁴⁷ Die reine Verwaltungstätigkeit der Nachrichtendienste ist mangels Grundrechtsrelevanz aus dem Kontrollgegenstand ausgenommen.

⁴⁸ Vgl. [Teil 1 B. III.](#)

6. Verhaltensnormen

Verhaltensnormen richten sich im Gegensatz dazu an den Kontrollierten und beinhalten rechtliche Vorgaben und Folgen für dessen Verhalten.⁴⁹ Die Befugnisnormen sind die wichtigsten Verhaltensnormen. Die Befugnisnormen aller Nachrichtendienste sowie deren Tatbestandsvoraussetzungen und -grenzen detailliert zu vergleichen, übersteigt den Rahmen der Dissertation. Einen Überblick liefert jedoch die Darstellung der den Nachrichtendiensten übertragenen Aufgaben und insbesondere die typisierende Analyse der ihnen verliehenen Befugnisse.⁵⁰

7. Kontrollergebnis

Das Kontrollergebnis ist, was aus der Anlegung des Kontrollmaßstabs an den Kontrollgegenstand folgt. Entweder wird die sich aus dem Maßstab ableitende Eigenschaft, hier die Frage, ob ein Verhalten „rechtmäßig“ ist, bejaht oder verneint. Die Konsequenzen, die an ein beliebiges Ergebnis gebunden sind, nennt *Kempny* „Kontrollergebnisfolgen“. Einzelne Kontrollergebnisse zu analysieren, ist nicht das Ziel der Ausarbeitung. Die normativ vorgesehenen und möglichen Kontrollergebnisfolgen werden jedoch aufgeschlüsselt.

8. Kontrollverhältnis

Als Kontrollverhältnis bezeichnet *Kempny* die durch die Kontrollnormen geschaffene Beziehung, innerhalb derer die Kontrolle sich vollzieht. An ihr können mehrere Einheiten beteiligt sein. Das Kontrollverhältnis besteht jeweils zwischen den Datenschutzbeauftragten, G 10-Kommissionen und dem UKRat als Kontrolleuren und den Nachrichtendiensten und deren übergeordneten Behörden als Kontrollierten. Übergeordnete Behörde des BfV ist das Bundesinnenministerium, des BND das Bundeskanzleramt und des MAD das Verteidigungsministerium. Auf der Landesebene sind die jeweiligen Innenministerien die den Verfassungsschutzbehörden übergeordneten Behörden. Die Aufsichtsbehörden der Nachrichtendienste des Bundes sind beispielsweise in die Kontrollen involviert, wenn der BfDI Datenschutzverstöße des Nachrichtendienstes beanstandet, da die Beanstandung „gegenüber der zuständigen obersten Bundesbehörde“ erfolgen muss.⁵¹

⁴⁹ Häufig werden diese Normen auch als „Handlungsnormen“ bezeichnet, *Kempny*, Verwaltungskontrolle, S. 22 f.

⁵⁰ Vgl. [Teil 1 B. II.](#)

⁵¹ §§ 27 Nr. 1 BVerfSchG, 16 Abs. 2 S. 1 BDSG; §§ 64 Nr. 1a BNDG, 16 Abs. 2 S. 1 BDSG; §§ 13 Nr. 1 MADG, 16 Abs. 2 S. 1 BDSG. In den meisten Bundesländern ist es identisch geregelt, vgl. [Teil 3 D. II. 6. a.](#)

9. Anwendung auf diese Untersuchung

Das Begriffswerkzeug von *Kempny* unterstützt dabei, den Untersuchungsgegenstand herauszuarbeiten. Unproblematisch bestimmen lassen sich einzig die Nachrichtendienste als *Kontrollierte* und die Rechtmäßigkeit als *Kontrollmaßstab*. Die *Kontrollleute* sind zwar einfach-rechtlich festgelegt und insofern identifizierbar, in Folge der Analyse ergibt sich jedoch, dass die Aufgabe des Kontrollleure teilweise anderen Institutionen zukommen sollte.⁵² Der *Kontrollgegenstand* sowie die *Verhaltensnormen* werden grob umrissen.⁵³ Das Hauptaugenmerk der Untersuchung liegt darauf, die *Kontrollnormen* zu beleuchten.⁵⁴ Während das Kontrollergebnis einzelfallbezogen sowie tatsächlicher Natur ist und daher nicht untersucht wird, sollen die denkbaren *Kontrollergebnisfolgen* dargestellt werden.

Das Modell von *Kempny* ist nicht auf eine Vielzahl von Kontrollierten und eine Mehrheit von Kontrollleuren ausgeweitet worden.⁵⁵ Die Begrifflichkeiten lassen sich dennoch übertragen, weil auch in der hier betrachteten Konstellation immer jeweils ein Kontrolleur (z.B. der BfDI) und ein Kontrollierter (z.B. das BfV) identifizierbar sind.

III. Maßstäbe für die Analyse und Bewertung von Kontrolle

Ein wichtiger Bewertungsmaßstab von Normen ist ihre Vereinbarkeit mit höherrangigem Recht. Zu prüfen, inwieweit die einfach-rechtlichen Regelungen zur Rechtskontrolle der Nachrichtendienste mit höherrangigem Recht vereinbar sind, ist ein zentrales Anliegen dieser Arbeit. Um die Untersuchung der Rechtskontrolle zu strukturieren, erfolgt sie unter Zuhilfenahme folgender ausgewählter verwaltungswissenschaftlicher Parameter:

1. Initiative

Um Kontrollsysteme analysieren zu können, bietet es sich zunächst an, danach zu fragen, von welcher Einheit die Kontrolle im Regelfall ausgeht.⁵⁶ In Betracht kommen neben dem Kontrolleur und dem Kontrollierten auch Dritte.⁵⁷ Solche Dritte sind beispielsweise potenziell Betroffene, die sich gem. § 15 Abs. 5 S. 1 Alt.2 G 10 mit einer

⁵² Vgl. [Teil 4 B.](#)

⁵³ Vgl. [Teil 1 B. II.](#)

⁵⁴ Vgl. [Teil 2, Teil 3.](#)

⁵⁵ Die Systembildung könnte „dergestalt fortgeführt werden, dass Kontrollmehrheiten in den Blick genommen würden. Dabei könnte insbesondere der Frage nachgegangen werden, inwieweit verschiedene Kontrollen einander wechselseitig beeinflussen und unter welchen Umständen sie einander ganz oder teilweise zu ersetzen vermögen“, *Kempny*, Verwaltungskontrolle, S. 282.

⁵⁶ *Kabl*, Kontrolle, 459, 485; *Schmidt-Aßmann*, Verwaltungskontrolle, 9, 14.

⁵⁷ *Schmidt-Aßmann*, Verwaltungskontrolle, 9, 14.

Beschwerde an die G 10-Kommission wenden können. Dann wird der Kontrolleur auf die Initiative des mutmaßlich betroffenen Dritten hin tätig.

2. Zeitpunkt

Darüber hinaus ist der Kontrollzeitpunkt relevant: Es gibt sowohl vorherige Kontrollen (ex ante), laufende bzw. begleitende Kontrollen als auch nachträgliche Kontrollen (ex post).⁵⁸

Bei der vorherigen Kontrolle existieren Alternativen und die behördliche Entscheidung ist noch nicht getroffen, während bei der nachträglichen Kontrolle geprüft wird, „ob die damalige Entscheidung richtig gewesen ist“. Die laufende Kontrolle „begleitet“ demgegenüber „die Durchführung einer Entscheidung“.⁵⁹

Die Vorabkontrolle hat den Vorteil, dass mitunter irreversible, ungerechtfertigte Grundrechtseingriffe im Vorhinein identifiziert und unterbunden werden können.⁶⁰ Daraus sollte jedoch nicht gefolgert werden, dass ex ante-Kontrollen im Nachrichtendienstrecht generell sinnvoller seien⁶¹, denn diese Bewertung lässt außer Acht, dass auf Seiten des Kontrollierten schutzwürdige Interessen gegen eine Vorabkontrolle existieren können, die berücksichtigt werden müssen. So verzögern Vorabkontrollen beispielsweise die Umsetzung der geplanten Maßnahme.⁶² Zudem liegen häufig die zur Prüfung der Rechtmäßigkeit im Einzelfall notwendigen Informationen erst nach dem Eingriff vor, was ex post-Kontrollen insoweit effektiver macht.⁶³ Es gibt daher keinen Kontrollzeitpunkt, der einem anderen abstrakt vorzuziehen wäre.

3. Modalität

Kontrollen können einmalig auf Grund eines spontanen Anlasses erfolgen oder in regelmäßigen Abständen auftreten (spontane und periodische Kontrollen), sie können aber auch dauerhafter Natur sein (permanente Kontrollen).⁶⁴

⁵⁸ Eichborn/Friedrich, Verwaltungsökonomie, S. 252; Hoffmann-Riem, Verwaltungskontrolle, 325, 346; Strößenreuther, Behördeninterne Kontrolle, S. 47 f.; als „Kontrollphasen“ bezeichnend: Kabl, Kontrolle, 459, 480; Armin, Kontrolle, 1316, 1317.

⁵⁹ Strößenreuther, Behördeninterne Kontrolle, S. 48.

⁶⁰ Bantlin, G 10-Kommission, S. 99.

⁶¹ Bantlin, G 10-Kommission, S. 99: „Eine vorheriger Kontrolle erweist sich somit im Hinblick auf die nachrichtendienstlichen Besonderheiten als besonders sinnvoll.“

⁶² Zu zeitlichen Kontrollbarrieren: Hoffmann-Riem, Verwaltungskontrolle, 325, 350; für besonders eingriffsintensive nachrichtendienstliche Mittel kann eine Vorabkontrolle auf der Grundlage höherrangigen Rechts dennoch angezeigt sein, vgl. BVerfG, Urteil v. 19.5.2020, 1 BvR 2835/17 Rn. 181, dazu ausführlich [Teil 2 A. III. 3. d.](#)

⁶³ Steiner, GSZ 2023, 124, 130.

⁶⁴ Kabl, Kontrolle, 459, 486; Schmidt-Aßmann, Verwaltungskontrolle, 9, 14.

4. Distanz

Dass zwischen den Kontrollierten und dem Kontrolleur eine gewisse Distanz gewahrt werden muss, weil diese den Vergleich und die Bewertung erst ermöglicht, ist unbestritten.⁶⁵ Diese Distanz kann mit Hilfe bestimmter organisatorischer Vorkehrungen selbst bei Eigenkontrollen (das heißt Kontrollen durch eine andere Einheit innerhalb derselben Behörde) gewahrt werden.⁶⁶

5. Kontrollmittel zur Informationsgewinnung

Kontrolle setzt denkbare Voraussetzungen voraus, dass der Kontrolleur über den zu kontrollierenden Vorgang informiert ist.⁶⁷ Auf diese Weise gelingt es dem Kontrolleur, der in der hier untersuchten Konstellation immer zugleich ein Außenstehender ist, den Ist-Wert zu erkennen, was ihn überhaupt erst zu dem angestrebten Vergleich befähigt.⁶⁸ Dementsprechend zentral ist es, dass ihm der Zugang zu zuverlässigen, vollständigen und aktuellen Informationen gewährt wird.⁶⁹ Denkbare Instrumente zur Informationsgewinnung sind beispielsweise Akteneinsichtsrechte, Zutrittsrechte zu Räumen des Kontrollierten, Befragungs- und Auskunftsrechte, Anzeige- und Berichtspflichten des Kontrollierten sowie Zustimmungsvorbehalte des Kontrolleurs.⁷⁰ Über Akteneinsichten Kenntnisse erlangen zu können, setzt voraus, dass behördenintern Akten angelegt, dass Vorgänge protokolliert und dokumentiert werden.⁷¹

Die genannten Informationsmittel überlassen dem Kontrollierten die Entscheidungsmacht darüber, was er mitteilen möchte. Deshalb fordern manche, dass der Informationszugang auch „ohne oder gegen den Willen“ des Kontrollierten eröffnet werden müsse.⁷²

⁶⁵ Schmidt-Aßmann, Verwaltungskontrolle, 9, 10; „Unabhängigkeit“ bei Armin, Kontrolle, 1316, 1317; Scheuner, Verantwortung und Kontrolle, 379, 392.

⁶⁶ „Kontroll-spezifische Distanz“, die personell, organisatorisch oder prozedural gewährleistet sein kann, vgl. Schmidt-Aßmann, Ordnungsidee, S. 229.

⁶⁷ Gusy, VerwArch 2015, 437, 443; Bantlin, G 10-Kommission, S. 92; Kahl, Kontrolle, 459, 545; Waldbhoff, Kontrolle, 73, 74.

⁶⁸ Bantlin, G 10-Kommission, S. 92.

⁶⁹ Kahl, Kontrolle, 459, 545.

⁷⁰ Schmidt-Aßmann, Verwaltungskontrolle, 9, 14; Hoffmann-Riem, Verwaltungskontrolle, 325, 352; Bantlin, G 10-Kommission, S. 92; zu Befragungs- und Auskunftsrechten (im Zusammenhang mit den Kompetenzen des PKGrG): Bartodziej, Hdb. des Rechts der Nachrichtendienste, 1533, 1572 ff.

⁷¹ Zu diesem Erfordernis auf die Nachrichtendienste bezogen: Singer, § 5 Rn. 18; Gusy weiterführend zu einer „Tendenz zur Informationszersplitterung“ innerhalb der Behörde, Gusy, VerwArch 2015, 437, 444; hinsichtlich der Datenschutzkontrolle der Zusammenarbeit von Polizei und Nachrichtendiensten im Gemeinsamen Terrorabwehrzentrum: Bergemann, Hdb. des Polizeirechts, 1225, 1295 Rn. 168.

⁷² Explizit zur parlamentarischen Kontrolle der Nachrichtendienste, Waldbhoff, Kontrolle, 73, 74.

Ein im Vergleich (nahezu) ungefilterter Eindruck des Ist-Zustandes kann mit Hilfe von Whistleblowern gelingen.⁷³ Whistleblower sind Mitarbeiter der kontrollierten Behörden, die Dritten über Interna berichten. Normen, die es ihnen ermöglichen, dem Kontrolleur solche Informationen mitzuteilen, sind aus der Perspektive einer funktionierenden Kontrollarchitektur sinnvoll, weil sie die Kenntnis des Kontrolleurs über die Tatsachengrundlage des Vergleichs vertiefen.⁷⁴

Darüber hinaus könnte man den Kontrolleur dazu berechtigen, im Rahmen der Kontrolle selbst Stichproben aus technischen Systemen zu entnehmen, ihm also einen direkten Zugriff auf Datenbestände zu gewähren.⁷⁵

6. Kontrollergebnisse

Wird Kontrolle so verstanden, dass ihr neben dem Vergleich die anschließende Einwirkung auf den Kontrollierten inhärent ist, muss überlegt werden, wie eine solche Einwirkung gestaltet werden kann. Denkbar sind zunächst Anreize für die Kontrollierten, wie zum Beispiel eine Belohnung durch Beförderung.⁷⁶ Auf externe Kontrollen lassen sich diese Anreiz-Instrumente allerdings nicht anwenden. Stattdessen können die Kontrolleure mit Rechtsgrundlagen für Sanktionen ausgestattet werden. Sanktionen sind die Möglichkeit zur Bußgeldverhängung, Fehlerkorrekturen durch Beanstandungen, die Erstellung von öffentlichen Berichten⁷⁷ und Stellungnahmen oder die Auferlegung von Berichtspflichten für den Kontrollierten.⁷⁸ Außerdem bestünde die Möglichkeit, dass der Kontrolleur den Kontrollierten schlicht auf Fehler hinweist oder ihn berät.⁷⁹

⁷³ Bantlin, G 10-Kommission, S. 94 ff.; Gusy, VerwArch 2015, 437, 443.

⁷⁴ Für die praktische Relevanz dieser Normen kommt es entscheidend darauf an, dass die Whistleblower vor strafrechtlichen Sanktionen und bestenfalls auch vor Bekanntmachung ihrer Identität geschützt werden, vgl. dazu Bantlin, G 10-Kommission, S. 95, 96.

⁷⁵ Den UN-Sonderberichterstatter für das Recht auf Privatsphäre zitierend und auf solche Regelungen in anderen europäischen Ländern hinweisend: Wetzling, Nachrichtendienstkontrolle.

⁷⁶ Kabl, Kontrolle, 459, 463 Rn. 7.

⁷⁷ Zu deren Bedeutung bei parlamentarischen Kontrollgremien: „Man wird insoweit darüber nachdenken müssen, den Kontrollinstanzen wenigstens das -eventuell verfahrensrechtlich eingeschränkte- Recht einzuräumen, jedenfalls in abstrahierter, die konkrete Aufgabenwahrnehmung nicht beeinträchtigender Weise etwaige Missstände im Parlament und der Öffentlichkeit mitzuteilen. Soll Kontrolle eine Bedeutung haben, ist es schwer vorstellbar, dass unliebsame Ergebnisse wie im Märchen als Geheimnis des Königs gehandelt werden müssen, die nur in ein Loch im Wald gerufen werden dürfen“, Masing, Nachrichtendienste, 3, 12.

⁷⁸ Schmidt-Aßmann, Ordnungsidee, S. 230; Gusy, VerwArch 2015, 437, 441; Hoffmann-Riem, Verwaltungskontrolle, 325, 352. Gusy bezeichnet auch die Kassation bestimmter Entscheidungen als Sanktion, vgl. Gusy, VerwArch 2015, 437, 441.

⁷⁹ Hoffmann-Riem, Verwaltungskontrolle, 325, 352.

7. Fachkompetenz

Eine wichtige Bedingung der Fremdkontrolle ist, dass der Kontrolleur das notwendige Fachwissen hat, um den Vergleich vornehmen zu können.⁸⁰ Für die Rechtskontrolle ist Rechtskenntnis allein meist nicht ausreichend, unter anderem kann zusätzlich technisches Sachverständnis⁸¹ unverzichtbar sein.

8. Kontrolltiefe

Der Umfang und die Genauigkeit eines Kontrollvorgangs werden maßgeblich dadurch beeinflusst, wie detailliert die maßgeblichen Verhaltensnormen ausgestaltet sind, deren Beachtung kontrolliert werden soll.⁸² Dort, wo Kontrolle nicht nur dem objektiven Rechtsschutz dient, sondern auch subjektive Rechte schützen soll, kann eine Detailkontrolle „unverzichtbar“ sein.⁸³ Wie intensiv Kontrollen ausgestaltet sein sollten, lässt sich pauschal nicht bestimmen, weil es dafür zusätzlich auf die Aufgaben des Kontrollierten und den institutionellen Rahmen ankommt, in dem die Kontrolle stattfindet.⁸⁴

9. Klare Kontrollstrukturen

Damit Kontrollen funktionieren können, ist es wichtig, dass die Kompetenzen unterschiedlicher Kontrolleure eindeutig voneinander abgegrenzt sind. Eine „unsichere oder umstrittene“ Aufteilung von Kontrollkompetenzen könnte zu „überflüssige[n] oder schädliche[n]“ Doppel- und Mehrfachkontrollen, Reibungsverlusten und Ressourcenverschwendung führen.⁸⁵ Unklare Kontrollstrukturen könnten zudem „Desorientierung“ und „Rechtsunsicherheit“ beim Kontrollierten hervorrufen.⁸⁶

10. Kontrollniveau

Für die Bewertung der Kontrolle kommt es darauf an, dass im Zusammenspiel mehrerer Kontrollmechanismen insgesamt ein „hinreichendes Kontrollniveau“ entsteht.⁸⁷

⁸⁰ *Arnim*, Kontrolle, 1316, 1317; *Hoffmann-Riem*, Verwaltungskontrolle, 325, 350; dies bezüglich der G 10-Kommission verneinend, *Bantlin*, G 10-Kommission, S. 159.

⁸¹ Vgl. beispielsweise BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 285: „informationstechnische Kenntnisse“ erforderlich.

⁸² *Kabl*, Kontrolle, 459, 482; *Gusy*, VerwArch 2015, 437, 450 f.

⁸³ Beispielhaft die Datenschutzkontrolle durch die Datenschutzbeauftragten anführend: *Hoffmann-Riem*, Verwaltungskontrolle, 325, 348.

⁸⁴ Ebd.

⁸⁵ *Kabl*, Kontrolle, 459, 548.

⁸⁶ Ebd. bezogen auf die Kontrolle öffentlicher Unternehmen. Es spricht nichts dagegen, diesen Gedanken auf die Verwaltung als Kontrollierten zu übertragen.

⁸⁷ *Schmidt-Aßmann*, Ordnungsidee, S. 213.

Statt den Blick auf einzelne Kontrollinstanzen zu verengen und einseitig deren Kontrollfähigkeit auszubauen, soll das im Zusammenwirken mit anderen Kontrolleuren entstehende additive Kontrollniveau mitgedacht werden.⁸⁸

Da diese Untersuchung sich auf die Rechtskontrolle durch externe Stellen beschränkt, kann das Kontrollniveau nicht für das Zusammenspiel aller Kontrollmechanismen untersucht werden. Ob eine solche Betrachtungsweise der Nachrichtendienstkontrolle möglich wäre, muss bezweifelt werden. Dagegen sprechen die unterschiedlichen Zwecke der politischen Kontrolle und der Rechtskontrolle⁸⁹, die es ausschließen, die unterschiedlichen Kontrollarten miteinander zu verrechnen.⁹⁰ Die nachträgliche gerichtliche Kontrolle kann in das Kontrollniveau nicht einbezogen werden, weil sie wegen ihrer praktisch verschwindend geringen Bedeutung im Nachrichtendienstrecht aus der Untersuchung ausgeklammert ist⁹¹.

Die Forderung, das additive Kontrollniveau zu betrachten und zu beachten, lässt sich trotzdem für die Rechtskontrolle fruchtbar machen, da die externe Rechtskontrolle ihrerseits von mehreren Kontrolleuren ausgeübt wird (Datenschutzbeauftragte, G 10-Kommissionen und UKRat).

11. Barrieren

Es gibt verschiedene Faktoren, die kontrollbegrenzend wirken können. Rechtliche Barrieren können sich beispielsweise aus der Aufgabenbeschreibung der am Kontrollverhältnis Beteiligten oder der Aufteilung von Zuständigkeiten im Föderalismus ergeben. Außerdem sind kontrollbegrenzende Normen zum Schutz der nationalen Sicherheit oder der Vertraulichkeit denkbar.

Die Kontrolle kann auch aus psychologischen Gründen erschwert sein, wenn etwa das Misstrauen gegenüber dem Kontrolleur zu groß ist („Misstrauenswall“). Umgekehrt besteht die Gefahr einer Fraternisierung von Kontrolleur und Kontrollierten (sog. „agency capture“⁹²).⁹³

⁸⁸ Ebd.

⁸⁹ Vgl. [Teil 1 A. I. 2.](#)

⁹⁰ Gusy, VerwArch 2015, 437, 441.

⁹¹ Vgl. [Teil 1 A. I. 4.](#)

⁹² „One can also mention here the phenomenon of ‘agency capture’, (...) whereby a body established to monitor and control a regulatory agency is gradually drawn within the sphere of influence of the agency and becomes its spokesman rather than its watchdog.“, Cameron, National Security, S. 167.

⁹³ So auch Venedig-Kommission, Report 2007, Rn. 223: “There is a danger that these judges become so used to the types of techniques, information and assessments they see every day that they lose their qualities of independence and external insight through a process of acclimatisation“; drastisch formuliert bei Wetzling/Dietrich, Disproportionate use of commercially and publicly available data, S. 38, die vom Risiko eines „accountability theatre“ sprechen.

Möglich ist zudem, dass die Kontrollierten wesentlich und uneinholbar mehr wissen als der Kontrolleur (sog. kognitive Kontrollbarriere). In Situationen, in denen eine Behörde schnell reagieren muss, kann Kontrolle an der Eilbedürftigkeit scheitern (sog. zeitliche Kontrollbarriere). Die Kontrollreichweite kann überdies dadurch begrenzt sein, dass dem Kontrolleur zu wenig Personal oder Geld zur Verfügung steht oder die Kontrollmittel nicht ausreichend schlagkräftig ausgestaltet sind (Ressourcenbarrieren).⁹⁴

12. Effektivität und Effizienz

*Hoffmann-Riem*⁹⁵ erklärt, dass Verwaltungskontrolle auf ihre Effektivität und Effizienz hin zu untersuchen sei. Die Effektivität definiert er als einen „Zielerreichungsgrad innerhalb vorgegebener sozio-ökonomischer Rahmenbedingungen“, welcher anhand des anwendbaren Normzusammenhangs ermittelt werden müsse. Ein Instrument, Effektivität zu fördern, können Kontrollmittel sein.⁹⁶

Effizienz sei gegeben, wenn man das als effektiv ermittelte Ziel mit dem „dafür geringstmöglichen Ressourceneinsatz“ erreiche. Er führt weiter aus, dass Kontrolle „möglichst wenig Personaleinsatz bei Kontrolleuren und Kontrollierten erfordern sollte“ und dass auf die „Organisationsstruktur und Organisationskultur unter Einschluss der Führungs- und Kommunikationskultur Rücksicht“ zu nehmen sei, weshalb die personellen Ressourcen auch „mit Blick auf Motivation, Kreativität“ und „Leistungskraft über die Zeit“ zu „schonen“ seien. Die Kontrolle müsse insoweit optimiert werden, dass sie ein „zumutbares“ Maß erreicht. Eine Möglichkeit, die Effizienz zu steigern, besteht darin, Kontrollen selektiv zu gestalten. Auf diese Weise werden zugleich personelle Ressourcen des Kontrolleurs geschont und der Arbeitsaufwand für den Kontrollierten gesenkt. Dahinter steht die Überlegung, dass die bloße Möglichkeit von Kontrollen das Verwaltungshandeln in eine Richtung lenken kann, die die Kontrolle überflüssig macht.⁹⁷

⁹⁴ Für den gesamten Absatz: *Hoffmann-Riem*, Verwaltungskontrolle, 325, 349 f., der darauf hinweist, dass Kontrollbarrieren nicht per se „dysfunktional“ sind, sondern ggf. der Herausbildung eines „angemessenen“ Kontrollgefüges dienen; *Wetzling/Vieth*, Gute Rechtsnormen und innovative Kontrollpraxis, S. 83.

⁹⁵ In diesem Absatz zitiert: *Hoffmann-Riem*, Verwaltungskontrolle, 325, 345 f.; die Begriffe als Kriterien erwähnend: *Kahl*, Kontrolle, 459, 475.

⁹⁶ M. w. N.: *Schmidt-Aßmann*, Verwaltungskontrolle, 9, 41.

⁹⁷ *Hoffmann-Riem*, Verwaltungskontrolle, 325, 354; zur Wirkung von Protokollierungspflichten, *Wetzling*, Nachrichtendienstkontrolle.

13. Kontrolllexzesse

Kontrolllexzesse durch die Kontrolleure sollten vermieden werden. Ein Kontrolllexzess ist eine Situation, in der der Kontrolleur unmittelbar für und anstelle der Kontrollierten entscheidet. Er sollte vermieden werden, weil er die Eigenständigkeit des Kontrollierten gefährdet.⁹⁸ Begründet wird diese Forderung damit, dass die (kontrollierte) Handlung im Verantwortungsbereich des Kontrollierten liege und dort verbleiben soll („eigene Verantwortungssphären“).⁹⁹ Dafür spricht zudem, dass Kontrolle besser gelingt, wenn sie vom Kontrollierten als „hilfreiche Dienstleistung“ empfunden wird und der Kontrolleur nicht gegen einen „Misstrauenswall“ auf Seiten des Kontrollierten ankämpfen muss.¹⁰⁰

B. Nachrichtendienste als Kontrollierte

Die vorangegangenen Ausführungen sind der Einführung in die Rechtskontrolle gewidmet. Die nun folgenden dienen dazu, die Nachrichtendienste, welche die Position des Kontrollierten einnehmen, in den Fokus zu rücken.¹⁰¹ Dazu werden in einem ersten Schritt die Gesetzgebungs- und Verwaltungskompetenzen dargestellt, da die Organisation der Kontrollinstitutionen daran anknüpft.¹⁰² Zudem werden die Aufgaben der einzelnen Behörden erörtert und voneinander abgegrenzt. Anschließend sollen die Befugnisse der Nachrichtendienste und damit deren Verhaltensnormen schlaglichtartig umrissen werden. Im Modell von *Kempny* gesprochen, sollen demnach der „Kontrollierte“, der „Kontrollgegenstand“ und die „Verhaltensnormen“ herausgearbeitet werden.

I. Staatsrechtliche Verortung

Welche Gebietskörperschaft für die Rechtsgrundlagen und die Ausführung der Nachrichtendienste zuständig ist, ergibt sich aus einer Gesamtschau der Art. 70 ff. GG mit den Art. 83 ff. GG.

⁹⁸ *Kahl*, Kontrolle, 459, 546; *Bantlin*, G 10-Kommission, S. 102 f.

⁹⁹ *Hoffmann-Riem*, Verwaltungskontrolle, 325, 349.

¹⁰⁰ *Hoffmann-Riem*, Verwaltungskontrolle, 325, 351.

¹⁰¹ Das Militärische Nachrichtenwesen ist aus der Untersuchung ausgeklammert, weil es gesetzlich nicht geregelt ist.

¹⁰² So auch *Venedig-Kommission*, Report 2015, Rn. 68: "(...) states differ as to how they organise their security functions and this is an important part of the context of oversight, as the oversight arrangements track the way the security function is organised."

1. Verfassungsschutz des Bundes

Gem. Art. 71, 73 Abs. 1 Nr. 10 GG ist der Bund zuständig für die Gesetzgebung im Bereich der „Zusammenarbeit“ des Bundes und der Länder zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes (lit. b) und zum Schutz vor Bestrebungen im Bundesgebiet, die auswärtige Belange gefährden (lit. c). Da die ausschließliche Bundeszuständigkeit somit auf die „Zusammenarbeit“ beschränkt ist, handelt es sich beim Verfassungsschutz um eine „geteilte Aufgabe von Bund und Ländern“¹⁰³. „Zusammenarbeit“ im Sinne der Norm ist die dauerhafte Kooperation zur gegenseitigen Unterrichtung, Auskunftserteilung, Beratung, Unterstützung und Hilfeleistung, die es den Behörden innerhalb der jeweiligen Befugnisse erlaubt, funktionell und organisatorisch verbunden zu sein sowie gemeinsame Einrichtungen und Informationssysteme zu betreiben.¹⁰⁴

Die Verwaltungskompetenz für die Einrichtung der Bundesverfassungsschutzbehörde wird aus Art. 87 Abs. 1 S. 2 GG hergeleitet.¹⁰⁵ Dieser Kompetenztitel berechtigt den Bund dazu, Zentralstellen einzurichten, die der Sammlung von Unterlagen für die Zwecke des Verfassungsschutzes und des Schutzes gegen gewalttätige oder Gewalt vorbereitende Bestrebungen im Bundesgebiet dienen.¹⁰⁶

Welche Funktionen und Befugnisse können dieser Zentralstelle übertragen werden? Je nachdem, wie die Art. 73 Abs. 1 Nr. 10 GG und Art. 87 Abs. 1 S. 2 GG ausgelegt werden und ihr Zusammenhang interpretiert wird, kommt man zu unterschiedlichen Ergebnissen. Teilweise wird angenommen, die beiden Normen ergänzten einander.¹⁰⁷ Das bedeutet, der Bund kann eine Zentralstelle einrichten, die im Rahmen der „Zusammenarbeit“ über Befugnisse verfügt, unabhängig davon aber ebenfalls operativ handeln darf.

Demgegenüber wird argumentiert, dass Art. 71 Abs. 1 Nr. 10 GG die Reichweite von Art. 83 Abs. 1 S. 2 GG als „äußerste Grenze“ determiniere. Die zweitgenannte Norm könne ihre Wirkung nur im Rahmen der Gesetzgebungskompetenz entfalten, sie aber nicht erweitern. Deshalb umfasse der Auftrag der Zentralstelle alles zur Kooperation notwendige, schließe abseits der Zusammenarbeit aber eigene Befugnisse des Bundesamtes aus.¹⁰⁸

¹⁰³ Bäcker, GSZ 2018, 213, 215; Gärditz, EuGRZ 2018, 6, 15.

¹⁰⁴ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn 97; BVerfG, Beschluss v. 10.11.2020 - 1 BvR 3214/15 - Rn. 76.

¹⁰⁵ Kornblum, Rechtsschutz, S. 44; Droste, Verfassungsschutzrecht, S. 36.

¹⁰⁶ Dazu, warum es sich beim BfV trotz der Bezeichnung als Bundesoberbehörde in § 2 Abs. 1 BVerfSchG (auch) um eine Zentralstelle handelt, Dürig/Herzog/Scholz/Ibler, Art. 87 GG Rn. 146; Gröpl, Nachrichtendienste, S. 138 f., 149.

¹⁰⁷ Vgl. Hecker, Hdb. des Rechts der Nachrichtendienste 2017, 222, 232 Rn. 16; Linzbach/Gärditz, ZG 2020, 314, 326.

¹⁰⁸ Bäcker, DöV, 840, 843 f.

Ogleich es für die Zwecke dieser Arbeit nicht erforderlich ist, die Problematik erneut¹⁰⁹ im Detail aufzufächern, ergibt sich aus der knappen Darstellung der widerstrebenden Interpretationen jedenfalls folgende Schlussfolgerung: Über die kompetenzrechtlichen Grenzen des Bundesverfassungsschutzes gibt es in der Wissenschaft keinen Konsens. In der Rechtspraxis hingegen hat sich der Gesetzgeber längst für den erstgenannten Standpunkt entschieden. Gestützt auf die Art. 73 Abs. 1 Nr. 10 GG, Art. 87 Abs. 1 S. 2 GG hat er das BfV eingerichtet, dem gem. §§ 8 ff. BVerfSchG unabhängig von Kooperationsaufgaben eigene Befugnisse zur Verfügung stehen.

2. Landesverfassungsschutz

Der Bund ist für die Zusammenarbeit von Bund und Ländern zwar ausschließlich zuständig, abgesehen davon ist der Verfassungsschutz aber Ländersache.¹¹⁰ Um die Länderkompetenz bestimmen zu können, ist die Auslegung des Begriffs der „Zusammenarbeit“ entscheidend. Legt man die oben genannte Definition des Bundesverfassungsgerichts von der Zusammenarbeit als ständiger Kooperation zugrunde, stellt man fest, dass das BfV dafür eines Kooperationspartners bedarf. Aus dem Bundesverfassungsschutzgesetz, das der Bundesgesetzgeber auf der Grundlage seiner Kompetenz gem. Art. 71 Abs. 1 Nr. 10 GG erlassen hat, ergibt sich die Pflicht der Länder, eine eigene Verfassungsschutzbehörde zu betreiben oder dies mit anderen Bundesländern gemeinsam zu tun (§ 2 Abs. 2 BVerfSchG).¹¹¹ Gem. den §§ 3, 6 Abs. 1 und 2 BVerfSchG gibt der Bundesgesetzgeber den Landesgesetzgebern zudem einen Mindestaufgabenkatalog vor. Dies wird damit begründet, dass eine Zusammenarbeit unmöglich wäre, wenn die Behörden nicht wenigstens einen „Kernbestand“ gemeinsamer Aufträge teilen.¹¹²

Abgesehen davon ist die gesetzliche Ausgestaltung Ländersache. Das bedeutet vor allem, dass die Landesgesetzgeber die Organisation ihrer Verfassungsschutzbehörden,

¹⁰⁹ Vgl. die Darstellung bei *Gröpl*, Nachrichtendienste, S. 134 ff.; *Bäcker*, DöV 2011, 840, 843 f.

¹¹⁰ BVerfG, Beschluss v. 24.5.2005 - 1 BvR 1072/01 - Rn. 62; *Dürig/Herzog/Scholz/Uhle*, Art. 73 GG Rn. 235; *Gröpl*, Nachrichtendienste, S. 114 f.

¹¹¹ BT-Drs. 10/4737, Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, des Verwaltungsverfahrensgesetzes, des Bundesverfassungsschutzgesetzes und des Straßenverkehrsgesetzes v. 28.1.1986, S. 50, 51; *Schenke/Graulich/Ruthig/Roth* § 2 BVerfSchG Rn. 14; *Brenner*, Bundesnachrichtendienst, S. 16; *Gröpl*, Nachrichtendienste, S. 88.

¹¹² *Schenke/Graulich/Ruthig/Roth*, § 2 BVerfSchG Rn. 14; *Gröpl* schreibt hingegen, dass eine einfachrechtliche Verpflichtung der Länder durch den Bund nicht erforderlich sei, weil sich dieselben Aufgaben wie für den Bund für die Länder ebenfalls aus Art. 73 Abs. 1 Nr. 10 GG ergäben. Der „verfassungsrechtliche Befehl“ adressiere die Länder gleichermaßen, vgl. *Gröpl*, Nachrichtendienste, S. 93 f.

die Aufgaben (jenseits des Pflichtkatalogs), die Befugnisse und die Zusammenarbeit mit anderen Verfassungsschutzbehörden unabhängig gestalten können.¹¹³

3. *Militärischer Abschirmdienst*

Dass dem Bund für den MAD die ausschließliche Gesetzgebungszuständigkeit zukommt, ergibt sich aus dem Kompetenztitel des Bundes für die „Verteidigung“ gem. Art. 73 Abs. 1 Nr. 1 GG. Die entsprechende Verwaltungskompetenz des Bundes folgt aus Art. 87a Abs. 1 S. 1 GG.¹¹⁴ Eine Folge dieser Kompetenzgrundlage ist, dass die Tätigkeit des MAD immer einen Bezug zur Landesverteidigung aufweisen muss.¹¹⁵

4. *Bundesnachrichtendienst*

Der Zuständigkeitskatalog in den Art. 70 ff. GG enthält – wie bereits hinsichtlich des MAD keinen speziellen Kompetenztitel für den Auslandsnachrichtendienst. Stattdessen wird die ausschließliche Zuständigkeit des Bundes auf die „auswärtigen Angelegenheiten“ in Art. 73 Abs. 1 Nr. 1 GG gestützt.¹¹⁶

Daraus ergibt sich, dass der Bund eine Stelle „mit aufgabenadäquaten Befugnissen“ zur Auslandsaufklärung schaffen darf. Wegen der übrigen Gesetzgebungskompetenzen des Bundes und der Länder sind die potenziellen Aufgaben einer solchen Stelle beschränkt: sie kann nicht bei jeglichem Auslandsbezug zuständig sein, sondern nur für Aspekte, „die für das Verhältnis der Bundesrepublik zu anderen Staaten oder zwischenstaatlichen Einrichtungen, insbesondere für die Gestaltung der Außenpolitik Bedeutung haben“. Die Aufgaben und Befugnisse des BND müssen daher stets eine „außen- und sicherheitspolitische Bedeutung“, eine „internationale Dimension“ haben. Die „primäre Aufgabe“ der Auslandsaufklärung ist, die Regierung über außen- und verteidigungspolitische Belange zu informieren. Solange das „Gesamtprofil“ seiner Tätigkeit von dieser Aufgabe geprägt ist, kann der BND auch mit der Früherkennung von aus dem Ausland drohenden Gefahren betraut werden, wenn diese sich auf die Stellung der Bundesrepublik in der Staatengemeinschaft auswirken können.¹¹⁷

Die Verwaltungskompetenz des Bundes für den BND folgt aus Art. 87 Abs. 3 GG.¹¹⁸

¹¹³ Überwiegend vertretene Auffassung, vgl. *Gröpl*, Nachrichtendienste, S. 114 f.; denkbar wäre die Formulierung von „rahmenartigen“ Mindeststandards durch den Bund auch für Befugnisse, vgl. *Bäcker*, Hdb. des Polizeirechts, 109, 145 f. Rn. 235.

¹¹⁴ *Bäcker*, Hdb. des Polizeirechts, 109, 146 Rn. 236; *Gröpl*, Nachrichtendienste, S. 78 f.

¹¹⁵ *Bäcker*, Hdb. des Polizeirechts, 109, 146 Rn. 237.

¹¹⁶ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 195 ff.; BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 122 ff.; *Dürig/Herzog/Scholz/Uhle*, Art. 73 GG Rn. 41.

¹¹⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 122 ff., 127.

¹¹⁸ *Bäcker*, DöV 2011, 840, 841; *Brenner*, Bundesnachrichtendienst, S. 40.

II. Gesetzliche Aufträge

Die Aufgaben der Nachrichtendienste ergeben sich aus dem jeweiligen Fachgesetz, welches auf der Grundlage der Gesetzgebungskompetenzen erlassen wurde.

1. Gemeinsamkeiten

Allen Nachrichtendiensten ist gemeinsam, dass sie Informationen über mögliche Bedrohungen sammeln sollen.¹¹⁹ Ein wesentlicher Unterschied liegt jedoch im Ursprung der Bedrohung: Während der BND aus dem Ausland stammende Bedrohungen identifizieren soll (Auslandsnachrichtendienst), sind die Verfassungsschutzbehörden für Gefährdungslagen zuständig, die ihre Ursache im Landesinnern haben oder sich innerhalb der Grenzen auswirken (Inlandsnachrichtendienst).¹²⁰ Die Bedrohung soll nachrichtendienstübergreifend so früh wie möglich erkannt werden. Deshalb erfolgt die Kerntätigkeit der Nachrichtendienste zu einem Zeitpunkt, in dem eine Gefahr noch nicht eindeutig benannt werden kann, sondern sich erst formiert.¹²¹

a. Politische Information

Die im Rahmen dieser Gefahrenfrüherkennung bzw. „Vorfeldaufklärung“ gesammelten Informationen sollen anschließend ausgewertet und an die Bundes- oder Landesregierung übermittelt werden, denn ein erster wesentlicher Zweck der Informationssammlung durch die Nachrichtendienste ist es, die politische Führung mit Lageberichten und Analysen zu versorgen („politische Information“¹²²).¹²³

¹¹⁹ Bächer, Hdb. des Verfassungsrechts, 1715, 1722; Warg, Hdb. des Rechts der Nachrichtendienste, 509, 513 Rn. 1; näher zum „Intelligence Cycle“ Bareinske, Hdb. des Rechts der Nachrichtendienste, 865, 881 f.

¹²⁰ Banzhaf, Präventionsbehörden, S. 120 ff.; „Primärzweck“ und „Sekundärzweck“ auch bei Tanneberger, Sicherheitsverfassung, S. 333; ähnlich Poscher/Rusteberg, KJ 2014, 57, 64, 68, wonach der Zweck des Verfassungsschutzes ausschließlich in der politischen Information bestehe.

¹²¹ Warg, Hdb. des Rechts der Nachrichtendienste, 509, 517 Rn. 7; F. Schneider, ZD 2021, 360, 361; zum Verfassungsschutz: Droste, Verfassungsschutzrecht, S. 176.

¹²² Bächer, Hdb. des Polizeirechts, 109, 205 Rn. 259 ff.

¹²³ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 118; Bergemann, Hdb. des Polizeirechts, 1225, 1113; Banzhaf, Präventionsbehörden, S. 78, Gusy bezeichnet sie als „Informationsdienstleister“, vgl. Gusy, Reformperspektiven, 19, 26; Poscher/Rusteberg, KJ 2014, 57, 62; Bächer, Eingriffstatbestände, 137, 147; dabei handele es sich um die „primäre, aber nicht mehr die einzige Aufgabe der nachrichtendienstlichen Auslandsaufklärung“, Barczak, KritV 2021, 91, 102.

b. Gefahrenfrüherkennung

Umstritten ist, ob auch die Gefahrenfrüherkennung (gleichrangige) Aufgabe aller Nachrichtendienste sein kann.

aa) Bundesnachrichtendienst

Für den BND hat das Bundesverfassungsgericht diese Frage eindeutig bejaht: Neben der primären Aufgabe der Regierungsinformation könne der BND auch mit der Früherkennung von aus dem Ausland drohenden Gefahren betraut werden, wenn diese von außen- und sicherheitspolitischer Bedeutung sind.¹²⁴

bb) Bundesamt für Verfassungsschutz und Militärischer Abschirmdienst

Zum BfV und zum MAD hat sich das Bundesverfassungsgericht allerdings bisher nicht entsprechend geäußert.

Für den Verfassungsschutz wird zum Teil unter anderem aus systematischen Erwägungen angenommen, er sei nicht mit der Gefahrenfrüherkennung betraut: Im ersten Abschnitt des Bundesverfassungsschutzgesetzes zu den Aufgaben des Verfassungsschutzes werde dieser nur mit der Informationssammlung beauftragt, wohingegen die Informationsübermittlung an die Strafverfolgungs- und Polizeibehörden erst im dritten Abschnitt, im Rahmen der Übermittlungsvorschriften, normiert sei. Die Mitwirkung bei der operativen Gefahrenabwehr sei gesetzessystematisch gerade nicht als Aufgabe festgelegt und erfolge nur im Einzelfall. Dafür spreche auch, dass für die Übermittlung an Gefahrenabwehr- und Strafverfolgungsbehörden eine Zweckänderung erforderlich ist. Daher sei eine „Einbindung der Ämter in Gefahrenabwehr und Strafverfolgung im BVerfSchG lediglich in zweiter Linie angelegt“.¹²⁵

Obwohl diese an der einfach-rechtlichen Ausgestaltung orientierten Erwägungen für sich genommen überzeugen, erscheint diese Auslegung der Gesetze praxisfern. Eine Vielzahl von Autoren, die über Kontakte in die Nachrichtendienste verfügen, messen dem Beitrag der Nachrichtendienste an der Gefahrenabwehr und Strafverfolgung ein höheres Gewicht bei: So seien die Nachrichtendienste „funktional sehr wohl an der Abwehr konkreter Gefahren bzw. Aufklärung von Straftaten beteiligt“.¹²⁶ Teilweise wird

¹²⁴ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 127 f.; *Barczak*, KritV 2021, 91, 104.

¹²⁵ *Banzhaf*, Präventionsbehörden, S. 120 ff.; „Primärzweck“ und „Sekundärzweck“ auch bei *Tanneberger*, Sicherheitsverfassung, S. 333; ähnlich *Poscher/Rusteberg*, KJ 2014, 57, 64, 68, wonach der Zweck des Verfassungsschutzes ausschließlich in der politischen Information bestehe.

¹²⁶ *Warg*, Hdb. des Rechts der Nachrichtendienste, 509, 518 Rn. 8; so auch *Unterreitmeier*, AöR 2019, 234, 276 ff., 291, 293; derselbe in *Unterreitmeier*, GSZ 2018, 1, 3 ff.; *Gärditz*, EuGRZ 2018, 6, 8 f.;

angenommen, das Bundesverfassungsgericht habe die Aufgabe der Gefahrenfrüherkennung neben dem BND auch für die anderen Nachrichtendienste anerkannt, da es im zweiten Antiterrorurteil feststellt, dass die Nachrichtendienste „nicht notwendig auf die politische Vorfeldaufklärung beschränkt“ seien.¹²⁷ Die zweitgenannte Ansicht ist mit den einfach-rechtlichen Rechtsgrundlagen vereinbar, da die Gesetze den Auftrag zwar als Sammlung und Auswertung von Information beschreiben, in den Auftragsnormen aber nicht festgelegt ist, an wen die Information zu richten ist. Darüber hinaus wäre der weit verstandene Auftrag verfassungsrechtlich grundsätzlich unproblematisch.¹²⁸ Allerdings müssen die Eingriffsschwellen der nachrichtendienstlichen Befugnisse angehoben werden, soweit die Nachrichtendienste neben der politischen Information zur Gefahrenfrüherkennung tätig werden (Konsequenz aus dem grundrechtlichen Trennungsgebot).¹²⁹

Anders als teilweise angenommen, hat das Bundesverfassungsgericht die Gefahrenfrüherkennung als Aufgabe der Verfassungsschutzbehörden jedoch bisher nicht anerkannt und sich diesen Überlegungen nicht angeschlossen. Der im zweiten Urteil zur Antiterrorurteil formulierte Hinweis darauf, dass die Tätigkeit der Nachrichtendienste nicht notwendig auf die Vorfeldaufklärung beschränkt sei, wurde in darauffolgenden Entscheidungen nicht aufgegriffen. Stattdessen formuliert das Bundesverfassungsgericht für Übermittlungen vom Verfassungsschutz an andere Sicherheitsbehörden hohe Anforderungen, weil mit der Übermittlung zu Gefahrenabwehr- oder Strafverfolgungszwecken eine Zweckänderung verbunden sei.¹³⁰ Aus der Notwendigkeit zur Zweckänderung folgt, dass das Bundesverfassungsgericht die Gefahrenabwehr und Strafverfolgung grundsätzlich als aufgabenfremd erachtet.

Der Gesetzgeber könnte die Aufgaben der Verfassungsschutzbehörden einfach-rechtlich um diesen Aspekt erweitern. Falls auch die Schwellen für Übermittlungen an

Linzbach/Gärditz, ZG 2020, 314, 335: „Einen Nachrichtendienst, der allein der politischen Regierungsberatung dienen würde, ohne einen realen Sicherheitsbeitrag leisten zu können, würde niemand mit Befugnissen zu eingriffsintensiven Überwachungsmaßnahmen ausstatten“; *Wolff*, DVBl 2015, 1076, 1078; zum BND *Dietrich*, GSZ 2020, 173, 175; vgl. auch die zusammengefasste Stellungnahme der bayerischen Landesregierung in BVerfG, Beschluss v. 10.11.2020 - 1 BvR 3214/15 - Rn. 47: „Die im Urteil zum Antiterrorurteilgesetz von 2013 vorgenommene Typisierung der Aufgaben und Befugnisse von Polizei und Verfassungsschutz sei zu überdenken [Anm: BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 118]. Tatsächlich bestünden erhebliche Überschneidungen der Aufgabenbereiche.“; ebenso die bayerische Landesregierung in BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 232.

¹²⁷ Mit Verweis auf BVerfG, Beschluss v. 10.11.2020 - 1 BvR 3214/15 - Rn. 104, *Barczak*, KritV 2021, 91, 104.

¹²⁸ *Bäcker*, Hdb. des Polizeirechts, 109, 152 Rn. 252.

¹²⁹ Vgl. [Teil 1 B. II. 2. b.](#)

¹³⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 232 ff.; 253 ff., BVerfG, Beschluss v. 28.9.2022 - 1 BvR 2354/13 - Rn. 124 ff.

Gefahrenabwehr- und Strafverfolgungsbehörden abgesenkt werden, müssten die Eingriffsschwellen der Befugnisse angehoben werden.

Über die Aufgaben des MAD hatte das Bundesverfassungsgericht bisher nicht zu entscheiden, die Ausführungen sind wegen seiner Tätigkeit als „Verfassungsschutzbehörde der Bundeswehr“ jedoch auf ihn übertragbar.

2. Zusammenarbeit mit Gefahrenabwehr- und Strafverfolgungsbehörden

Mit den Polizei- und Strafverfolgungsbehörden existieren zusätzlich zu den Nachrichtendiensten weitere Sicherheitsbehörden, deren Aufträge von denen der Nachrichtendienste abzugrenzen sind.

a. Klassische Abgrenzung

Zur Differenzierung wird grundsätzlich der Beginn des behördlichen Tätigwerdens angeführt: Während die Nachrichtendienste zur Früherkennung von einzelfallübergreifenden Bedrohungslagen – bereits im Vorfeld konkretisierter Gefahren – agieren dürfen, beginnen die Polizeibehörden ihre Tätigkeit erst zu einem späteren Zeitpunkt, um die Gefahren abzuwehren, die sich im Einzelfall mit einer gewissen Wahrscheinlichkeit realisieren werden oder um Straftaten zu verfolgen, falls die Gefahr sich schon in einen Schaden materialisiert hat.¹³¹ Wichtig ist, dass diese Abgrenzung auf den Beginn des behördlichen Tätigwerdens abstellt, nicht aber auf die gesamte Handlung, denn die nachrichtendienstliche Tätigkeit endet nicht abrupt, sobald eine Gefahr absehbar ist. In der Praxis sind diese Phasen allerdings nicht eindeutig differenzierbar.¹³²

b. Trennungsgebot und informationelles Trennungsprinzip

Grundsätzlich sollen die Nachrichtendienste einerseits sowie die Gefahrenabwehr- und Strafverfolgungsorgane andererseits miteinander kooperieren und ihr Wissen – im gesetzlich geregelten Rahmen – austauschen. Die Grenzen dieser Kooperation definiert das sog. Trennungsgebot. Wegen seiner Normierung in allen Verfassungsschutzgesetzen¹³³, dem MADG¹³⁴ und dem BNDG¹³⁵ errichtet das Trennungsgebot de

¹³¹ Bäckers, Hdb. des Verfassungsrechts, 1715, 1719 ff. Rn. 10, 11, 22.

¹³² Nehm, NJW 2004, 3289, 3292 f; Zöller, JZ 2007, 763, 767; Vgl. [Teil 1 B. II. 2. c.](#)

¹³³ Unterschiede gibt es jedoch im Detail, da teilweise die organisatorische, teilweise die kompetenzielle Trennung normiert wurde: Art. 5 Abs. 2 [BayVSG](#); §§ 2 Abs. 3, 5 Abs. 3 [BWLVS](#); § 2 Abs. 2 [LVerfSchG RP](#); § 1 Abs. 2 [HVS](#); § 2 Abs. 1 [VSG NRW](#); § 5 [NVerfSchG](#); § 2 Abs. 2 [HmbVerfSchG](#); § 2 Abs. 1 [BremVerfSchG](#); § 2 Abs. 2 [LVerfSchG SH](#); § 2 Abs. 1 [VSG Bln](#); § 2 Abs. 1 [BbgVerfSchG](#); § 2 Abs. 2 [VerfSchG MV](#); § 2 Abs. 2 [ThürVerfSchG](#); § 1 Abs. 3 [SächsVSG](#); § 2 Abs. 2 [VerfSchG-LSA](#); § 2 Abs. 1, 2 [SVerfSchG](#).

¹³⁴ § 1 Abs. 4 MADG.

¹³⁵ § 2 Abs. 3 BNDG.

lege lata¹³⁶ eine Barriere zwischen den Nachrichtendiensten einerseits und den Polizei- und Strafverfolgungsbehörden andererseits. Das auf den sog. Polizeibrief der Alliierten zurückgehende Trennungsgebot besagt, dass zwischen den Nachrichtendiensten und den Polizeibehörden organisatorisch unterschieden werden muss und die sich unterscheidenden Aufgaben nicht in einer Behörde gebündelt werden dürfen.¹³⁷ Außerdem arbeiten Mitarbeiter in der Regel ausschließlich in der einen oder der anderen Behörde.¹³⁸ Nach dem einfach-rechtlichen Trennungsgebot dürfen den Nachrichtendiensten gesetzlich keine imperativen Befugnisse verliehen werden, ihr Auftrag ist die Information.¹³⁹ Nur die Gefahrenabwehr- und Strafverfolgungsbehörden sollen den Bürgern (erkennbar) gegenüberreten, nur aus ihrem Handeln sollen direkte Konsequenzen folgen können.

Darüber hinaus kann sich aus der Verhältnismäßigkeit „reflexhaft“ ein grundrechtliches Trennungsgebot¹⁴⁰ ergeben. Soweit die Nachrichtendienste nach ihren einfach-rechtlichen Aufgaben und Befugnissen anders als die Gefahrenabwehr- und Strafverfolgungsorgane nicht an der operativen Gefahrenabwehr beteiligt sind, sind die Folgen ihrer Eingriffe als weniger schwerwiegend und der Eingriff damit insgesamt als milder einzustufen. Deshalb können ihre Maßnahmen unter niedrigeren Voraussetzungen erlaubt werden, als es bei vergleichbaren Instrumenten im Polizei- und Strafverfolgungsrecht verfassungsrechtlich zulässig wäre (sog. „verfassungsrechtliches Privileg der Nachrichtendienste“). Wenn und soweit den Nachrichtendiensten unter geringeren Schwellen weitgehendere Befugnisse verliehen werden, folgt daraus, dass ihre Tätigkeiten wirksam von denen anderer Sicherheitsbehörden getrennt werden müssen. Verzichtet der Gesetzgeber auf dieses Privileg, ist auch die Trennung hinfällig.¹⁴¹

¹³⁶ Gusy, GSZ 2021, 142, 144.

¹³⁷ Nehm, NJW 2004, 3289, 3290.

¹³⁸ Gusy, GSZ 2021, 142, 148.

¹³⁹ Im Polizeibrief zu den Nachrichtendiensten: „This agency shall have no police authority“, m. w. N. bei Bantlin, G 10-Kommission, S. 45; Poscher/Rusteberg, KJ 2014, 57, 58; Dietrich, Hdb. des Rechts der Nachrichtendienste, 249, 274 Rn. 36; Bäcker, Eingriffstatbestände, 137, 148.

¹⁴⁰ Vgl. zum verfassungsrechtlichen Streit um das „Trennungsgebot“ unter anderem Linzbach/Gärditz, ZG 2020, 314; Gusy, GSZ 2021, 142, 144; Nehm, NJW 2004, 3289, 3290 f.

¹⁴¹ Bäcker, Hdb. des Polizeirechts, 109, 150 Rn. 245 a, b, 154 Rn. 255 ff.; zustimmend Banzhaf, Präventionsbehörden, S. 123; im Ergebnis ähnlich Linzbach/Gärditz, ZG 2020, 314, 332, 335, wonach von dem Trennungsgebot nichts anderes übrig bliebe als ein im Kern aus der Verhältnismäßigkeit folgendes Umgehungsverbot, das die Autoren allerdings anders als Bäcker nicht als Trennungsgebot („semantische Anachronismen“) bezeichnen.

Das Bundesverfassungsgericht hat überdies in seiner Rechtsprechung aus dem Recht auf informationelle Selbstbestimmung ein „informationelles Trennungsprinzip“¹⁴² abgeleitet: Demnach sind Datenübermittlungen zwischen den genannten Behörden zwar nicht ausgeschlossen, müssen aber – hinsichtlich der Nutzung nachrichtendienstlicher Informationen durch Polizeibehörden – einem herausragenden öffentlichen Interesse bzw. einem „besonders wichtigen Rechtsgut“ dienen. Der Austauschvorgang soll gesetzlich präzise ausgestaltet und an qualifizierte Eingriffsschwellen („konkretisierte Gefahr“) gebunden sein, um zu verhindern, dass die Grenzen der Befugnisse einzelner Behörden durch Nutzbarmachen der Erkenntnisse einer anderen Sicherheitsbehörde außer Kraft gesetzt werden und auf diese Weise der datenschutzrechtliche Zweckbindungsgrundsatz missachtet wird.¹⁴³

Vor dem Hintergrund des grundrechtlichen Trennungsgebots ist eine solche informationelle Trennung richtigerweise nur so lange notwendig, wie die Nachrichtendienste ausschließlich mit der politischen Information betraut sind und deshalb über niedrigere Eingriffsschwellen verfügen; soweit sie zur Gefahrenfrüherkennung eingesetzt werden *und* die Tatbestandsvoraussetzungen ihrer Befugnisse entsprechend an die der Gefahrenabwehrbehörden angeglichen wurden, würde die informationelle Trennung entfallen.¹⁴⁴ Allerdings hat das Bundesverfassungsgericht die Gefahrenfrüherkennung als Aufgabe für den Verfassungsschutz bisher nicht anerkannt¹⁴⁵, sodass das informationelle Trennungsprinzip weiterhin maßgeblich bleibt. Das gilt im Übrigen auch für den BND, da dessen Aufgabe sich zwar auf die Gefahrenfrüherkennung erstreckt, seine Befugnisse aber weiterhin niedrigschwellig anwendbar sind.

c. Annäherung der Tätigkeiten und verstärkte Kooperation

Die organisatorische Trennung zwischen den Behörden existiert weiterhin, den Nachrichtendiensten wurden keine Zwangsbefugnisse verliehen¹⁴⁶. Trotzdem ist erkennbar, dass Rechtsetzungs- und Verwaltungspraxis eine Annäherung der Tätigkeitsfelder erwirkt haben. Dies betrifft vor allem die Aufgaben der Polizeibehörden und der Nachrichtendienste. Der Beobachtungsauftrag der Verfassungsschutzbehörden erstreckt

¹⁴² Zur Unterscheidung vom bis heute im Detail umstrittenen Trennungsgebot und dem „neuen“ Trennungsprinzip: *Gusy*, GSZ 2021, 142.

¹⁴³ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 123; BVerfG, Beschluss v. 10.11.2020 - 1 BvR 3214/15 - Rn. 105; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 253 ff.; BVerfG, Beschluss v. 28.9.2022 - 1 BvR 2354/13 - Rn. 124 ff.; *Bergemann*, Hdb. des Polizeirechts, 1225, 1257.

¹⁴⁴ Dann gilt nur der Grundsatz der hypothetischen Datenneuerhebung, *Bäcker*, Hdb. des Polizeirechts, 109, 156 f., 260 f.

¹⁴⁵ Vgl. [Teil 1 B. II. 1. b. bb\)](#).

¹⁴⁶ BVerfG, Beschluss v. 10.11.2020 - 1 BvR 3214/15 - Rn. 104.

sich auf die Beobachtung terroristischer Bestrebungen und mitunter auf die Beobachtung der Organisierten Kriminalität¹⁴⁷, obwohl es sich dabei um Straftaten handelt, deren Verhütung eine klassische Polizeiaufgabe ist. Darüber hinaus endet die Zuständigkeit des Verfassungsschutzes nicht, „wenn ein Bedrohungsszenario vom Vorfeld in eine Gefahr übergeht“, wodurch Situationen entstehen können, in denen sowohl der Verfassungsschutz als auch die Polizei zuständig sind.¹⁴⁸ Die Polizeibehörden wiederum werden einzelfallübergreifend, weit im Vorfeld einer konkreten Gefahr, eingesetzt.¹⁴⁹

Auch auf der Ebene der Instrumentarien, die die Behörden nutzen können, sind Gemeinsamkeiten identifizierbar. Denn neben den originär präventiv-polizeilichen Standardmaßnahmen oder originär repressiven Strafverfolgungsbefugnissen gibt es einen wachsenden Kanon an strukturell vergleichbaren Befugnisnormen in den Polizei- und Verfassungsschutzgesetzen.¹⁵⁰

Außerdem ist die informationelle Kooperation zwischen den Sicherheitsbehörden ausgebaut worden. Mit der Antiterrordatei betreiben die Nachrichtendienste, die Bundespolizei, die Landeskriminalämter, das Zollkriminalamt und das Bundeskriminalamt beispielsweise eine gemeinsame Datenbank, auf die im Rahmen der Terrorismusabwehr von allen Beteiligten zugegriffen werden kann, §§ 1 Abs. 1, 5 ATDG.¹⁵¹ Seit 2004 gibt es ein gemeinsames Terrorabwehrzentrum (GTAZ), in dem Vertreter der genannten Behörden, des Bundesamts für Migration und Flüchtlinge sowie ein Mitarbeiter des Generalbundesanwalts damit beauftragt sind, zur Terrorismusabwehr einen „schnellen und unmittelbaren Austausch von Information“ zu forcieren und Fachwissen zu bündeln.¹⁵² In Thüringen ist die Landesverfassungsschutzbehörde sogar verpflichtet, in Kooperation mit dem Landeskriminalamt wöchentlich einen Lagebericht über „Bestrebungen“ zu formulieren.¹⁵³

Die Entwicklung hin zu einer stärkeren Interferenz der Tätigkeitsbereiche wird im Schrifttum als „Vernachrichtendienstlichung“ der Polizei und „Verpolizeilichung“ der

¹⁴⁷ Bäcker, Hdb. des Verfassungsrechts, 1715, 1726 Rn. 34; Gusy, Grundrechte und Verfassungsschutz, S. 124; Löffelmann, GSZ 2018, 85, 86.

¹⁴⁸ Gusy, KritV 1994, 242, 245.

¹⁴⁹ Poscher/Rusteberg, KJ 2014, 57, 61; Bäcker, Hdb. des Verfassungsrechts, 1715, 1723 Rn. 23.

¹⁵⁰ Vgl. Gusy, Grundrechte und Verfassungsschutz, S. 126 f.

¹⁵¹ Dietrich, Hdb. des Rechts der Nachrichtendienste, 249, 276 Rn. 41; ein weiteres Beispiel sind gemeinsame Projektdaten, vgl. Zöller, JZ 2007, 763, 768.

¹⁵² https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/gtaaz-flyer.pdf?__blob=publicationFile&v=1 (abgerufen am 31.8.2024); formale Trennung aber in die polizeiliche Informations- und Analysestelle (PIAS) und die Nachrichtendienstliche Informations- und Analysestelle (NIAS), vgl. Zöller, JZ 2007, 763, 767 f.

¹⁵³ § 4 Abs. 5 ThürVerfSchG: „Das Amt für Verfassungsschutz und das Landeskriminalamt haben wöchentlich und anlassbezogen ein gemeinsames Lagebild über Bestrebungen im Sinne des Absatzes 1 zu erstellen. Zu diesem Zweck führen sie Informationen in der Thüringer Informations- und Auswertungszentrale zusammen.“

Nachrichtendienste umschrieben.¹⁵⁴ Nicht verfassungsrechtlich rechtfertigungsbedürftig wäre die Konvergenz der Tätigkeiten dann, wenn sich aus der einfach-rechtlichen Ausgestaltung der Fachgesetze ergibt, dass das nachrichtendienstliche Privileg aufgehoben wurde.¹⁵⁵ „Reflexhaft“ existiert dann auch das grundrechtliche Trennungsgebot nicht. Dann stellt sich jedoch die Frage, ob es sinnvoll ist, zwei Präventionsbehörden mit teilweise identischen Aufgaben vorzusehen. Alternativ könnte beispielsweise der Verfassungsschutz in den polizeilichen Staatsschutz integriert werden.

3. Auftrag der Verfassungsschutzbehörden

Die Bedrohungen, denen sich die Aufklärungsarbeit der Verfassungsschutzbehörden widmet, sind ursprünglich solche, die der freiheitlichen demokratischen Grundordnung drohen (vgl. § 1 Abs. 1 BVerfSchG).¹⁵⁶ Dieses Schutzgut ist deshalb der Ausgangspunkt für die Tätigkeit der Nachrichtendienste. Das Bundesverfassungsgericht beschrieb es in einem Parteiverbotsverfahren 1952 wie folgt: Die freiheitliche demokratische Grundordnung ist eine Ordnung,

*„(...) die unter Ausschluß jeglicher Gewalt- und Willkürherrschaft eine rechtsstaatliche Herrschaftsordnung auf der Grundlage der Selbstbestimmung des Volkes nach dem Willen der jeweiligen Mehrheit und der Freiheit und Gleichheit darstellt. Zu den grundlegenden Prinzipien dieser Ordnung sind mindestens zu rechnen: die Achtung vor den im Grundgesetz konkretisierten Menschenrechten, vor allem vor dem Recht der Persönlichkeit auf Leben und freie Entfaltung, die Volkssouveränität, die Gewaltenteilung, die Verantwortlichkeit der Regierung, die Gesetzmäßigkeit der Verwaltung, die Unabhängigkeit der Gerichte, das Mehrparteienprinzip und die Chancengleichheit für alle politischen Parteien mit dem Recht auf verfassungsmäßige Bildung und Ausübung einer Opposition.“*¹⁵⁷

¹⁵⁴ Bächer, Hdb. des Verfassungsrechts, 1715, 1726 Rn. 34; Bächer, Hdb. des Polizeirechts, 109, 152 Rn. 249 ff.; Löffelmann, GSZ 2018, 85, 86; Dietrich, Hdb. des Rechts der Nachrichtendienste, 249, 257 Rn. 8 m.w.N.; treffend auch die Beschreibung bei Gusy: „Die organisatorische Trennung blieb prinzipiell: die funktionelle Trennung schwand partiell. Überspitzt läßt sich formulieren: ‚Funktionell wuchs zusammen, was organisatorisch nicht zusammengehört.‘“, Gusy, KritV 1994, 242, 245.

¹⁵⁵ Bächer, Hdb. des Polizeirechts, 109, 153 Rn. 245.

¹⁵⁶ Herzog, Auftrag, 1, 8; Warg, Hdb. des Rechts der Nachrichtendienste, 509, 547 Rn. 46.

¹⁵⁷ BVerfG, Urteil v. 23.10.1952 - 1 BvB 1/51 - Rn. 37, vgl. auch BVerfG, Urteil v. 17.1.2017 - 2 BvB 1/13 - Rn. 529 ff.

Diese Formel ist in die Verfassungsschutzgesetze aufgenommen (vgl. z.B. § 4 Abs. 2 BVerfSchG) und detailliert worden.

a. Bundesamt für Verfassungsschutz

§ 3 BVerfSchG definiert den Auftrag des Bundesamts für Verfassungsschutz, adressiert aber auch die Landesverfassungsschutzbehörden. Die Kern-Aufträge der Landesverfassungsschutzbehörden werden demnach entsprechend den verfassungsrechtlichen Vorgaben bundeseinheitlich vorgegeben.¹⁵⁸ Sie ergeben sich aus § 3 Abs. 1 BVerfSchG, welcher originär eigene Aufgaben aufzählt und werden ergänzt in § 3 Abs. 2 BVerfSchG, der für bestimmte Konstellationen eine Mitwirkungspflicht gegenüber anderen öffentlichen Stellen etabliert.

aa) Eigene Aufgaben

Zunächst unterscheidet § 3 Abs. 1 BVerfSchG vier Aufträge.

(1) § 3 Abs. 1 BVerfSchG

Gem. § 3 Abs. 1 Nr. 1 BVerfSchG sollen Informationen über Bestrebungen gesammelt und ausgewertet werden, die gegen die freiheitliche demokratische Grundordnung (Alt. 1), den Bestand (Alt. 2) und die Sicherheit (Alt. 3) des Bundes oder eines Bundeslands gerichtet sind oder die Amtsführung von Verfassungsorganen oder Mitgliedern derselben beeinträchtigen wollen (Alt. 4).

Der Bestand des Bundes oder eines Bundeslandes (Alt. 2) umfasst gem. § 4 Abs. 1 Nr. 1 lit. a BVerfSchG drei Aspekte: Er meint erstens die Freiheit von fremder Herrschaft, zweitens die staatliche Einheit und drittens die Verhinderung von Gebietsabtrennungen. Der erste Aspekt, die Freiheit von fremder Herrschaft, beinhaltet die völkerrechtliche Souveränität und Unabhängigkeit sowie die faktische Unabhängigkeit gegenüber fremden Gewalten. Die staatliche Einheit bezieht sich auf die bundesstaatliche Struktur und deren Funktionsfähigkeit. Mit dem Begriff der „Gebietsabtrennung“ wird die Abspaltung einzelner Länder oder von Teilgebieten des Bundes umschrieben.¹⁵⁹

¹⁵⁸ BT-Drs. 10/4737, Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, des Verwaltungsverfahrensgesetzes, des Bundesverfassungsschutzgesetzes und des Straßenverkehrsgesetzes v. 28.1.1986, S. 51; Schenke/Graulich/Ruthig/Roth, §§ 3,4 BVerfSchG Rn. 5; Droste, Verfassungsschutzrecht, S. 86.

¹⁵⁹ Warg, Hdb. des Rechts der Nachrichtendienste, 509, 551 Rn. 52 ff.; Droste, Verfassungsschutzrecht, S. 191 f.; Schenke/Graulich/Ruthig/Roth, §§ 3,4 BVerfSchG Rn. 57.

Bestrebungen sind gegen die „Sicherheit“ (Alt. 3) gerichtet, wenn sie die Funktionsfähigkeit des Bundes oder eines Landes erheblich beeinträchtigen (vgl. § 4 Abs. 1 lit. b BVerfSchG). Erheblich ist die Beeinträchtigung, wenn sie „bedeutsame Belange der Allgemeinheit nachhaltig verletzt“.¹⁶⁰

(2) § 3 Abs. 1 Nr. 2, 3, 4 BVerfSchG BVerfSchG

Die Verfassungsschutzbehörden sollen darüber hinaus Spionagetätigkeiten anderer Staaten auf deutschem Territorium aufdecken, § 3 Abs. 1 Nr. 2 BVerfSchG.

Es sollen auch solche Bestrebungen identifiziert werden, die durch Gewalt oder vorbereitende Handlungen „auswärtige Belange“ gefährden, § 3 Abs. 1 Nr. 3 BVerfSchG. Ein „auswärtiger Belang“ ist gegeben, wenn auf die politische Ordnung in anderen Staaten aus dem Inland heraus gewalttätig eingewirkt wird und dies außenpolitische Interessen der Bundesrepublik gefährdet.¹⁶¹

Gegenstand der Aufklärung sind außerdem Bestrebungen, die gegen den Gedanken der Völkerverständigung oder des friedlichen Zusammenlebens der Völker gerichtet sind, § 3 Abs. 1 Nr. 4 BVerfSchG. Diese Tatbestandsalternative ist als Auffangnorm konzipiert.¹⁶²

(3) Bestrebungen

In § 3 Abs. 1 Nr. 1, 3, 4 BVerfSchG ist der Begriff der „Bestrebung“ zentral. Ausweislich der Legaldefinition in § 4 Abs. 1 lit. b, c BVerfSchG setzt dies einen „Personenzusammenschluss“ voraus, dessen Handeln entweder ziel- und zweckgerichtet die Funktionsfähigkeit des Bundes, der Länder oder ihrer Einrichtungen beeinträchtigt oder auf die Beseitigung eines Bestandteils der freiheitlich demokratischen Grundordnung gerichtet ist. Der „Personenzusammenschluss“ wird bejaht, wenn mindestens zwei Personen bei der Verfolgung eines der zuvor genannten Ziele zusammenarbeiten. Einzelne Personen sind grundsätzlich nicht von dem Begriff erfasst. Ausnahmsweise werden Individuen jedoch darunter subsumiert, wenn sie in ihrer Gefährlichkeit einer Gruppe von Personen ebenbürtig sind (§ 4 Abs. 1 S. 3 BVerfSchG). Gem. § 4 Abs. 1 S. 1 BVerfSchG wird einer Bestrebung zugerechnet, wer sie „nachdrücklich“ unterstützt. In welcher Form die Unterstützung erfolgt ist gleichgültig, soweit eine Erheblichkeitsschwelle

¹⁶⁰ *Warg*, Hdb. des Rechts der Nachrichtendienste, 509, 553 Rn. 55.

¹⁶¹ *Warg*, Hdb. des Rechts der Nachrichtendienste, 509, 558–562, der als Beispiele die Rekrutierung von im Ausland kämpfenden IS-Terroristen in Deutschland oder Anschläge auf ausländische Botschaften nennt; Schenke/Graulich/Ruthig/Roth, §§ 3, 4 BVerfSchG Rn. 73 ff.

¹⁶² BT- Drs. 14/7386, Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN v. 8.11.2001, S. 38; *Warg*, Hdb. des Rechts der Nachrichtendienste, 509, 559 ff.; Schenke/Graulich/Ruthig/Roth, §§ 3, 4 BVerfSchG Rn. 73 ff.

überschritten wurde. Eine weitere Voraussetzung ist, dass die Bestrebung auf eine Veränderung der politischen Ordnung hin ausgerichtet sein muss. Dabei kommt es auf eine subjektive Überzeugung nicht an. Ausreichend ist, dass der objektive Tatbestand von § 3 Abs. 1 BVerfSchG vorliegt.¹⁶³

Bestrebungen verfolgen ihre Ziele aktiv und müssen auf die „Durchsetzung eines politischen Ziels“ hin ausgerichtet sein, „dabei auf die Beeinträchtigung eines der Elemente der freiheitlichen demokratischen Grundordnung abzielen“ und darauf „hinarbeiten“. ¹⁶⁴

(4) Tatsächliche Anhaltspunkte

Alle Varianten des § 3 Abs. 1 BVerfSchG normieren tatsächliche Anhaltspunkte für ihr Bestehen als Voraussetzung für das Tätigwerden der Verfassungsschutzbehörden (§ 3 Abs. 1 S. 4 BVerfSchG). Das bedeutet, dass Tatsachen, die auf eine bestimmte Wahrscheinlichkeit der Tätigkeit oder Bestrebung hinweisen, zwar ausreichend sind, reine Vermutungen jedoch nicht genügen.¹⁶⁵

(5) Aufklärung der Gesellschaft

Eine weitere Aufgabe des BfV besteht darin, die Gesellschaft über Bedrohungen zu informieren¹⁶⁶ (§ 16 BVerfSchG). Dabei sind die Verfassungsschutzberichte das „zentrale Medium zur Unterrichtung der Öffentlichkeit über die Tätigkeiten der Verfassungsschutzbehörden“. ¹⁶⁷

bb) Problemfall organisierte Kriminalität

Ob darüber hinaus die Bekämpfung „organisierter Kriminalität“ ein Bestandteil des Verfassungsschutzauftrags gem. § 3 Abs. 1 BVerfSchG ist, ist umstritten. Ein wesentlicher Grund für die Unsicherheit zeigt sich bereits auf der gedanklich vorgelagerten

¹⁶³ Schenke/Graulich/Ruthig/Roth, §§ 3, 4 BVerfSchG Rn. 7–46; Warg, Hdb. des Rechts der Nachrichtendienste, 509, 533 ff.

¹⁶⁴ BVerwG, Urteil v. 14.12.2020 - 6 C 11/18 - Rn. 20 m.w.N., BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 185.

¹⁶⁵ BT- Drs. 14/7386, Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN v. 8.11.2001, S. 38; BVerwG, Urteil v. 17.10.1990 - 1 C 12/88; Warg, Hdb. des Rechts der Nachrichtendienste, 509, 525 Rn. 16.

¹⁶⁶ Banzhaf, Präventionsbehörden, S. 120; Brandt, Hdb. des Rechts der Nachrichtendienste, 1709, 1714, 1717 Rn. 7.

¹⁶⁷ Brandt, Hdb. des Rechts der Nachrichtendienste, 1709, 1715 Rn. 4.

Ebene¹⁶⁸: Bis heute existiert für den Begriff der „Organisierten Kriminalität“ in Rechtswissenschaft und -praxis keine einheitlich verwendete und kritikfreie Definition¹⁶⁹. Da für die Zwecke dieser Arbeit auf eine Präzisierung des Begriffs nicht verzichtet werden kann, wird eine Definition aus dem Jahr 1990 zugrunde gelegt.¹⁷⁰ Demnach ist organisierte Kriminalität:

„ (...) die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Zeit arbeitsteilig
a) unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,
b) unter Verwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder
c) unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken.“¹⁷¹

Diese Definition wird in der Literatur weiter begrenzt¹⁷²: Erstens sind terroristische Handlungen davon nicht erfasst. Zweitens scheiden Delikte der Wirtschaftskriminalität aus, sofern nicht zusätzlich die Varianten b) oder c) vorliegen.

Der Ursprung des Problems, ob es sich bei der Beobachtung organisierter Kriminalität um einen Verfassungsschutzauftrag handelt, liegt darin, dass der Begriff der organisierten Kriminalität im Wortlaut von § 3 Abs. 1 BVerfSchG nicht erwähnt wird. Ausgehend vom Wortlaut der Norm ist die Beobachtung organisierter Kriminalität somit keine Aufgabe der Verfassungsschutzbehörden. Dagegen, die organisierte Kriminalität unter § 3 Abs. 1 BVerfSchG zu subsumieren, spricht zudem, dass die Beweggründe für die Begehung von Delikten der organisierten Kriminalität überwiegend finanzieller Natur sind.¹⁷³ Mangels politisch bestimmter, zielgerichteter Verhaltensweise sind diese Strukturen häufig nicht mit den anderen in § 3 Abs. 1 Nr. 1 i. V. m. § 4 Abs. 1 S. 1 lit. a)

¹⁶⁸ So auch Gusy, StV 1995, 320, 321.

¹⁶⁹ Dazu ausführlich Lampe, Hdb. des Rechts der Nachrichtendienste, 781, 787 ff. Rn. 4.

¹⁷⁰ Dafür spricht, dass diese Definition sowohl in der Richtlinie für das Strafverfahren und Bußgeldverfahren (RiStBV) als auch in manchen Landesverfassungsschutzgesetzen rezipiert wurde, vgl. Lampe, Hdb. des Rechts der Nachrichtendienste, 781, 788 f. Rn. 4.

¹⁷¹ Schmitt/Köhler, StPO Anh 12 RiStBV Anl. E, S. 2545; Lampe, Hdb. des Rechts der Nachrichtendienste, 781-816, 789 Rn. 4; Schmitt/Köhler, Anh 12 RiStBV Anl E, S. 2545.

¹⁷² Lampe, Hdb. des Rechts der Nachrichtendienste, 781, 789 Rn. 4.

¹⁷³ Denninger, KritV 1994, 232-241, 234; Bergemann, Hdb. des Polizeirechts, 1225, 1244 Rn. 43; Hetzer, StV 1999, 165, 170 f.; Warg, Hdb. des Rechts der Nachrichtendienste, 509, 556 Rn. 60.

– c) BVerfSchG vorgesehenen Alternativen vergleichbar und somit nicht darunter subsumierbar.¹⁷⁴

Dennoch wird die Beobachtung organisierter Kriminalität teilweise für zulässig erachtet, weil die organisierte Kriminalität ein Ausmaß annehmen könne, bei dem unter anderem durch massive Korruption von Amtsträgern eine Gefährdung des Rechtsstaatsprinzips und der Funktionsfähigkeit des Staates vorstellbar sei.¹⁷⁵

Dem ist entgegenzuhalten, dass solche schwerwiegenden Erscheinungsformen organisierter Kriminalität im Einzelfall ohnehin unter die Tatbestandsvoraussetzungen von § 3 Abs. 1 BVerfSchG subsumiert werden können, weil die Voraussetzungen der Tatbestandsalternativen vorliegen, vor allem, wenn eine ungesetzhafte Beeinträchtigung der Amtsführung von Verfassungsorganen anzunehmen ist.¹⁷⁶

cc) Mitwirkungspflichten

Zu den originären Aufgaben der Verfassungsschutzbehörden gem. § 3 Abs. 1 BVerfSchG treten Mitwirkungspflichten gem. § 3 Abs. 2 BVerfSchG. „Mitwirkungspflicht“ bedeutet, dass die Verfassungsschutzbehörden nicht eigeninitiativ, sondern auf Ersuchen anderer öffentlicher Stellen tätig werden.¹⁷⁷ Der Verfassungsschutz prüft auf Basis dieser Rechtsgrundlage, ob Personen, die in lebens-, sicherheits- oder verteidigungspolitischen Einrichtungen beschäftigt werden (lit. b) oder denen geheimhaltungsbedürftige Tatsachen anvertraut werden sollen (lit. a), mangels Zuverlässigkeit oder aufgrund von Erpressbarkeit ein Sicherheitsrisiko darstellen, vgl. § 5 StGB. Der Verfassungsschutz ist demnach für den präventiven Geheim- und Sabotageschutz zuständig.¹⁷⁸

¹⁷⁴ Bergemann, Hdb. des Polizeirechts, 1225, 1244 Rn. 43; Hetzer, StV 1999, 165, 168; Gröpl, Nachrichtendienste, S. 356; Gusy argumentiert überzeugend mit dem Zweck der Schaffung des Verfassungsschutzes, der darin bestünde (noch) legale Handlungen aufzuklären, um Lücken zu schließen, die entstehen, weil legale Tätigkeiten außerhalb der Zuständigkeit der Polizei lägen. Organisierte Kriminalität „zeichnet sich aber gerade durch ihre Eigenschaften als Kriminalität, also durch ihre Illegalität aus“, weshalb mit den übrigen Aufgaben nicht vergleichbar sei, Gusy, KritV 1994, 242, 248.

¹⁷⁵ Droste, Verfassungsschutzrecht, S. 203 f.; Schenke/Graulich/Ruthig/Roth, §§ 3, 4 BVerfSchG Rn. 26; Werthebach/Droste-Lehnen, ZRP 1994, 57, 63 f.

¹⁷⁶ Bergemann, Hdb. des Polizeirechts, 1225, 1244 Rn. 43; Gusy, StV 1995, 320, 325; Hetzer, StV 1999, 165, 170.

¹⁷⁷ Schenke/Graulich/Ruthig/Roth, §§ 3, 4 BVerfSchG Rn. 144.

¹⁷⁸ Droste, Verfassungsschutzrecht, S. 142 f.

b. Landesämter für Verfassungsschutz

§ 3 BVerfSchG gilt bundesweit.¹⁷⁹ Dementsprechend haben die Landesgesetzgeber entweder den Wortlaut aus der Norm in ihre Landesverfassungsschutzgesetze übernommen¹⁸⁰ oder verweisen auf die Aufgabennorm im BVerfSchG¹⁸¹. Allerdings können die Landesgesetzgeber neben den bundesrechtlich vorgegebenen Aufgaben aus § 3 BVerfSchG weitere festlegen, denn bei den im BVerfSchG normierten Aufträgen handelt es sich lediglich um den Mindeststandard.¹⁸² Diesen landesrechtlichen Spielraum haben die Gesetzgeber in unterschiedlicher Intensität genutzt.

aa) Organisierte Kriminalität

In drei Landesverfassungsschutzgesetzen¹⁸³ erstreckt sich der gesetzliche Auftrag auf die Beobachtung von organisierter Kriminalität.¹⁸⁴ Der Begriff ist in den Gesetzen identisch definiert und entspricht der zitierten Begriffsbestimmung aus dem Jahr 1990. Die ausdrückliche Aufzählung im Aufgabenkatalog hat zur Folge, dass die organisierte Kriminalität auf Landesebene unabhängig von einem bestimmten Bedrohungspotenzial generell beobachtet werden kann.¹⁸⁵ Die Rechtslage unterscheidet sich damit von der auf Bundesebene, wo Erscheinungsformen organisierter Kriminalität nur im Einzelfall beobachtet werden können, soweit eine Tatbestandsalternative aus § 3 Abs. 1 BVerfSchG vorliegt.¹⁸⁶ Gegenüber den landesrechtlichen Auftragserweiterungen wird kritisch angemerkt, dass die generelle Beobachtung organisierter Kriminalität mit den klassischen Aufgaben des Verfassungsschutzes nicht vergleichbar sei und diese Normen

¹⁷⁹ Vgl. [Teil 1 B. II. 3 a.](#)

¹⁸⁰ § 3 [BWLVS](#)G; § 2 [HV](#)S; § 5 2 [LVerfSchG](#) RP; § 3 [NVerfSchG](#); § 4 [HmbVerfSchG](#); § 5 [LVerfSchG](#) SH; § 3 [BbgVerfSchG](#); § 5 [VerfSchG](#) MV; § 5 [VSG](#) Bln; § 4 [ThürVerfSchG](#); § 2 [SächsVSG](#); § 4 [VerfSchG](#)-LSA; § 3 [VSG](#) NRW; § 3 [SVerfSchG](#); § 3 [BremVerfSchG](#).

¹⁸¹ Art. 3 [BayVSG](#).

¹⁸² BT-Drs. 10/4737, Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, des Verwaltungsverfahrensgesetzes, des Bundesverfassungsschutzgesetzes und des Straßenverkehrsgesetzes v. 28.1.1986, S. 51; Schenke/Graulich/Ruthig/Roth, §§ 3, 4 BVerfSchG Rn. 5.

¹⁸³ Art. 3 S. 2 [BayVSG](#); § 2 Abs. 2 Nr. 5 [HV](#)S; § 3 Abs. 1 Nr. 4 [SVerfSchG](#); vgl. zur Entwicklung [Löffelmann/Zöller](#), Nachrichtendienstrecht, S. 95.

¹⁸⁴ [Warg](#), Hdb. des Rechts der Nachrichtendienste, 509, 556 Rn. 59.

¹⁸⁵ Beispielfhaft illustrierend aus S. 341 des Verfassungsschutzberichts Bayern (2020) zur „Russisch-eurasischen OK“, von der zu erwarten sei, dass sich immer mehr Mitglieder in Westeuropa und Deutschland niederlassen würden: „Bereits in den letzten Jahren konnten in Bayern immer wieder Aufenthalte von „Dieben im Gesetz“ festgestellt werden, die sich zum Teil auch zu medizinischen Behandlungen in Bayern aufhielten“, ähnlich Verfassungsschutzberichts Bayern (2023), S. 344; die Vereinbarkeit dieser Abkoppelung vom Aufklärungsauftrag aus § 3 BVerfSchG mit dem Trennungsgebot verneinend: [SächsVerfGH](#), NVwZ 2005, 1310, 1312.

¹⁸⁶ So auch [Banzhaf](#), Präventionsbehörden, S. 86; [Bergemann](#), Hdb. des Polizeirechts, 1225, 1245 Rn. 44.

verfassungskonform dahingehend ausgelegt werden müssten, dass die Voraussetzungen der klassischen Auftragsnormen dennoch gegeben sein müssen, dass also zugleich eine verfassungsfeindliche Bestrebung vorliegen muss.¹⁸⁷

Grundsätzlich können die Landesgesetzgeber ihren Verfassungsschutzbehörden weitere Aufgaben und Befugnisse verleihen, soweit eine wirksame Erfüllung der (Mindest-)Aufgaben gewährleistet bleibt und die Zusammenarbeit mit dem BfV nicht beeinträchtigt wird.¹⁸⁸ Keine dieser Konstellationen liegt hier vor. Dennoch dürfte eine Grenze erreicht sein. Die Ausweitung auf die Beobachtung von jeglichen Formen organisierter Kriminalität führt dazu, dass diese Landesämter auch zum Zweck der „Gefahrenfrüherkennung“ eingesetzt werden. Bisher hat das Bundesverfassungsgericht die „Gefahrenfrüherkennung“ als Aufgabe der Verfassungsschutzbehörden jedoch nicht anerkannt, sondern sie als aufgabenfremd behandelt.¹⁸⁹ Das spricht dafür, dass die Landesgesetze insoweit verfassungskonform ausgelegt werden müssen und die sonstigen Voraussetzungen von § 3 Abs. 1 BVerfSchG ebenfalls vorliegen müssen. Damit dürften diese Auftragsnormen kaum noch praktische Relevanz haben.¹⁹⁰

bb) Fortwirkende Strukturen der Deutschen Demokratischen Republik (DDR)

In weiteren zwei Verfassungsschutzgesetzen¹⁹¹ ist der Verfassungsschutz damit beauftragt, Informationen über fortwirkende Strukturen der Geheimdienste der DDR zu sammeln. Diese Vorschriften ergänzen die in § 3 Abs. 1 Nr. 2 BVerfSchG normierte Beobachtungspflicht von Spionagetätigkeiten anderer Staaten und verdeutlichen, dass die Behörden der DDR zwar aufgelöst sind, ihre Strukturen in den Geheimdiensten der Russischen Föderation jedoch fortwirken (könnten).¹⁹²

cc) Öffentlichkeitsaufklärung und Prävention

In allen Bundesländern und auf der Bundesebene gibt es Rechtsgrundlagen, die eine Veröffentlichung von Verfassungsschutzberichten vorschreiben.¹⁹³ Auf diese Weise

¹⁸⁷ Bergemann, Hdb. des Polizeirechts, 1225, 1245 Rn. 45; Vgl. auch VerfGH Sachsen, Urteil v. 21.7.2005 - Vf. 67-II-04 - Rn. 87 ff.; Löffelmann/Zöller, Nachrichtendienstrecht, S. 95.

¹⁸⁸ BVerwG, Beschluss v. 9.1.1995 - 1 B 231/94 - Rn. 8.

¹⁸⁹ Vgl. [Teil 1 B. II. 1. b. bb\)](#).

¹⁹⁰ Löffelmann/Zöller, Nachrichtendienstrecht, S. 96.

¹⁹¹ § 4 Abs. 1 Nr. 5 ThürVerfSchG; § 4 Abs. 1 Nr. 2 VerfSchG-LSA; die vergleichbare Regelung im sächsischen Verfassungsschutzgesetz wurde 2024 gestrichen, Gesetzesentwurf der Staatsregierung, Sächsischer Landtag, Drs. 7/15464, S. 18.

¹⁹² Warg, Hdb. des Rechts der Nachrichtendienste, 509, 555 Rn. 58a; vgl. auch Banzhaf, Präventionsbehörden, S. 85, der die eigenständigen Bedeutung dieser Kompetenzen als „gering“ einordnet.

¹⁹³ Brandt, Hdb. des Rechts der Nachrichtendienste, 1709, 1720 Rn. 14.

soll die Öffentlichkeit über die Arbeit der Verfassungsschutzbehörden und über aktuelle Entwicklungen informiert werden.

In manchen Landesgesetzen findet man darüber hinaus in den Auftragsnormen Formulierungen, welche die Öffentlichkeitsarbeit ausweiten. So heißt es teilweise, der Verfassungsschutz sei zur „Prävention“¹⁹⁴ verpflichtet, er solle Bestrebungen „durch Angebote zur Information“¹⁹⁵ entgegenwirken oder „Angebote zum Ausstieg“¹⁹⁶ eröffnen. Damit wird der ursprüngliche Auftrag der Informationsvermittlung an die Regierung und die Bürger um die Verpflichtung ergänzt, auf die Beobachtungsobjekte einzuwirken.

In Niedersachsen lautet die Begründung für die Einführung dieser Aufgabe, dass diese Art der Präventionstätigkeit aus dem Auftrag zur Öffentlichkeitsaufklärung abgeleitet werden könne und durch die Normierung die Gleichwertigkeit und Bedeutung dieses Auftrags betont werde.¹⁹⁷ Bemerkenswert hieran ist die Gleichsetzung zwischen der Öffentlichkeitsaufklärung einerseits und dem „Herantreten“¹⁹⁸ an Anhänger der Bestrebung andererseits trotz der damit verfolgten unterschiedlichen Zwecke. Die Öffentlichkeitsarbeit dient dazu, den Bestrebungen i. S. d. § 3 Abs. 1 BVerfSchG den Resonanzraum zu entwenden, einen Beitrag zur möglichst aufgeklärten, resilienten Gesellschaft zu schaffen und auf diese Weise die freiheitlich demokratische Grundordnung zu schützen.¹⁹⁹ Die Angebote an Szenemitglieder hingegen sollen Einzelne unterstützen, die extremistische Bestrebung zu verlassen. Die Gleichsetzungsargumentation verkennt, dass es zwischen Mitarbeiterinnen des Verfassungsschutzes, die sammeln, auswerten und informieren und solchen, die beobachteten Personen oder Personenzusammenschlüssen Informations- und Ausstiegsangebote machen, einen grundlegenden Unterschied gibt. Dieser besteht darin, dass sich anders als bei der Erweiterung des Beobachtungsauftrags auf die organisierte Kriminalität oder ehemalige Staatsicherheitsstrukturen nicht das beobachtete Objekt ändert, sondern die Tätigkeit der Behörde. Ob diese Art der Präventionstätigkeit noch mit dem Beobachtungsauftrag aus § 3 BVerfSchG vereinbar ist, ist fraglich. Legistisch erscheint es sauberer, den landesrechtlichen Beobachtungsauftrag um diese Aufgabe zu ergänzen.

¹⁹⁴ § 5 Abs. 2 [VerfSchG MV](#); § 5 Abs. 1 [ThürVerfSchG](#); § 4a [VerfSchG-LSA](#).

¹⁹⁵ § 3 Abs. 3 [NVerfSchG](#); § 5 Abs. 2 [ThürVerfSchG](#); § 3 Abs. 3 [VSG NRW](#); § 4a [VerfSchG-LSA](#).

¹⁹⁶ § 3 Abs. 3 [NVerfSchG](#); § 3 Abs. 3 [VSG NRW](#).

¹⁹⁷ Landtag Niedersachsen, Drs. 17/2161, Entwurf eines Gesetzes zur Neuausrichtung des Verfassungsschutzes im Land Niedersachsen v. 14.10.2014, S. 23.

¹⁹⁸ Ebd.

¹⁹⁹ Zum Verfassungsschutzbericht: *Brandt*, Hdb. des Rechts der Nachrichtendienste, 1709, 1717 Rn. 7.

4. Auftrag des Militärischen Abschirmdienstes

Der MAD ist die „Sonderverfassungsschutzbehörde“ der Streitkräfte.²⁰⁰ Seine Tätigkeit unterscheidet sich von der des Verfassungsschutzes in einem zentralen Aspekt: Der MAD beobachtet nur solche Bedrohungen, die den Geschäftsbereich des Verteidigungsministeriums betreffen (§ 1 Abs. 1 MADG).²⁰¹ Das Ziel des MAD besteht darin, die Mitarbeiter sowie die Einrichtungen der Bundeswehr vor „Unterwanderung, Zersetzung, Sabotage und Spionage“ zu schützen und die „Funktionsfähigkeit“ zu erhalten (Abschirmauftrag).²⁰² In dieser Funktion wirkt er bei der Sicherheitsüberprüfung von Mitarbeitern im Bereich des Verteidigungsministeriums mit (§ 1 Abs. 3 MADG). Darüber hinaus ist der MAD damit beauftragt, die Sicherheitslage deutscher und alliierter Streitkräfte im Ausland zu beurteilen, vgl. § 1 Abs. 2 Nr. 2 MADG.

5. Auftrag des Bundesnachrichtendienstes

Der BND sammelt Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, und wertet diese aus (§ 1 Abs. 2 BNDG). „Außenpolitik“ in diesem Sinne ist das Auftreten Deutschlands auf der Bühne der internationalen Beziehungen und seine Stellung in der Staatengemeinschaft; „Sicherheitspolitik“ ist die zweckorientierte Reaktion auf (abstrakte) Gefahren, die der Bundesrepublik von Außen drohen.²⁰³ Entgegen dem Wortlaut, der die außen- und sicherheitspolitische Wichtigkeit voraussetzt, ist es ausreichend, wenn eine der beiden Alternativen bejaht werden kann. Der „Aufklärungsauftrag“²⁰⁴ ist mit Blick auf diese Definitionen vielfältig und sehr weit gefasst: Zusätzlich zu Informationen über Gefahren aus dem Ausland, welche die Sicherheit von Bürgern oder die des Staates bedrohen, dürfen sämtliche Gegenstände in den Fokus gerückt werden, die für die außen- und sicherheitspolitischen Entscheidungen der Bundesregierung relevant sein können.²⁰⁵ Dies schließt beispielsweise auch wirtschaftliche Entwicklungen von sicherheitspolitischer Bedeutung ein. Die „organisierte Kriminalität“ ist nicht spezifisch genannt und daher nur vom Aufklärungsauftrag des Nachrichtendienstes erfasst, wenn sie unter die Voraussetzungen von

²⁰⁰ Vgl. *Bäcker*, Hdb. des Verfassungsrechts, 1715, 1722; *Gusy*, ApuZ 2014, 9, 13.

²⁰¹ *Hirsch*, Kontrolle, S. 33; *Gröpl*, Nachrichtendienste, S. 232 f.

²⁰² *Gröpl*, Nachrichtendienste, S. 232; Treffende Beschreibung des Auftrags bei *Gusy*: „nachrichtendienstlicher Selbstschutz der Bundeswehr gegen andere als militärische Gefahren“, *Gusy*, ApuZ 2014, 9, 13.

²⁰³ *Warg*, Hdb. des Rechts der Nachrichtendienste, 509, 571 Rn. 84.

²⁰⁴ *Schenke/Graulich/Ruthig/Gusy*, § 1 BNDG Rn. 23.

²⁰⁵ „Dieser Auftrag ist thematisch nahezu grenzenlos (...)“, *Bäcker*, Eingriffstatbestände, 137, 142.

§ 1 Abs. 2 BNDG subsumierbar ist. Ob die beobachteten Handlungen illegal oder legal sind, ist für die Arbeit des BND unerheblich.

Sein Auftrag ist nicht auf das Ausland begrenzt, vielmehr darf er auch innerhalb Deutschlands agieren, weil der Auslandsbezug in der Aufgabenbeschreibung nicht örtlich, sondern inhaltlich gemeint ist. Der BND handelt anders als der Verfassungsschutz unabhängig von „tatsächlichen Anhaltspunkten“ einer Gefahr, weshalb seine Tätigkeit im Vergleich noch weiter im Vorfeld beginnt.²⁰⁶

Der BND wirkt demnach im Ergebnis als „Sicherheitsdienstleister und außenpolitischer Ratgeber“²⁰⁷ der Bundesregierung. Die Bundesregierung detailliert den normativ weiten Auftrag in einem als Verschlussache eingestuften Auftragsprofil (APB) und bestimmt somit die Schwerpunkte der Aufklärungsarbeit.²⁰⁸

III. Befugnisse

Die Nachrichtendienste haben eine Vielzahl an Befugnissen, um ihre Aufgaben zu erfüllen. Dabei stehen ihnen vergleichbare Instrumente zur Verfügung, die sich aber in den Tatbestandsvoraussetzungen und Verfahrensregeln teilweise voneinander unterscheiden.²⁰⁹ Diese Unterschiede sollen im Folgenden nicht umfassend dargestellt werden.²¹⁰ Für die Untersuchung der Rechtskontrolle ist ein Grundverständnis für den Gegenstand der Rechtskontrolle ausreichend.

1. Überblick über die Art der Befugnisse

Zunächst soll in Kurzfassung dargestellt werden, welche Befugnisse die Nachrichtendienste jeweils auf der Basis welcher Ermächtigungsgrundlagen anwenden dürfen.

²⁰⁶ Warg, Hdb. des Rechts der Nachrichtendienste, 509, 570 ff. Rn. 84 f.; Schenke/Graulich/Ruthig./Gusy, § 1 BNDG Rn. 24 ff.; Gröpl, Nachrichtendienste, S. 221 ff.

²⁰⁷ Warg, Hdb. des Rechts der Nachrichtendienste, 509, 572 Rn. 85; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 128.

²⁰⁸ Bareinske, Hdb. des Rechts der Nachrichtendienste, 865, 919 f. Rn. 84.

²⁰⁹ Dem BVerfSchG kommt diesbezüglich dennoch eine „Leitfunktion“ zu, vgl. Bäcker, Eingriffstatbestände, 137, 138.

²¹⁰ Soweit ersichtlich, sind die Befugnisnormen aller Nachrichtendienste vergleichend noch nicht im Detail untersucht worden. Den Rahmen dieses Projekts würde dies weit überschreiten. Vgl. aber Löffelmann/Zöller, Nachrichtendienstrecht, S. 96 ff., 163 ff. sowie die Ausarbeitung auf der Metaebene bei Bäcker, Eingriffstatbestände, 137, ff.

a. Generalklausel zur Informationserhebung

Die Nachrichtendienste dürfen (personenbezogene) Informationen erheben, wenn es zur Aufgabenerfüllung erforderlich ist oder „tatsächliche Anhaltspunkte“ bzw. „Tatsachen“ ersichtlich sind, anhand derer anzunehmen ist, dass die Maßnahme Erkenntnisse über verfassungsschutzrelevante Bestrebungen, Tätigkeiten oder Quellen erbringen wird oder Mitarbeiter der Nachrichtendienste schützt (Generalklausel).²¹¹

Die Informationserhebung kann mit oder ohne den Einsatz von nachrichtendienstlichen Mitteln erfolgen.

Was nachrichtendienstliche Mittel sind, ist in § 8 Abs. 2 BVerfSchG exemplarisch aufgezählt: „Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden.“ In manchen Landesgesetzen sind die zulässigen nachrichtendienstlichen Mittel, die für verdeckte Datenerhebungen verwendet werden können, abschließend aufgezählt.²¹² Überwiegend kann jedoch für den Einsatz nachrichtendienstlicher Mittel auf die Generalklausel zurückgegriffen werden, soweit das Gesetz keine speziellen Rechtsgrundlagen für die jeweilige Maßnahme vorsieht.²¹³ Dementsprechend vermittelt die in diesem Kapitel angestrebte Aufführung der nachrichtendienstlichen Befugnisse nur für diejenigen Behörden ein vollständiges Bild ihrer Tätigkeit, deren verdeckte Befugnisse abschließend aufgezählt sind. Da grundrechtsinvasive Maßnahmen wegen des Wesentlichkeitsprinzips einer detaillierten Rechtsgrundlage bedürfen, ist davon auszugehen, dass die Generalklauseln nicht für eingriffsintensive Maßnahmen eingesetzt werden.²¹⁴

Für die Datenerhebungen ohne nachrichtendienstliche Mittel ist charakteristisch, dass sie keine Barrieren überwinden müssen oder berechtigtes Vertrauen enttäuschen, sie sind daher grundrechtsschonend und können grundsätzlich auf die Generalklausel

²¹¹ § 8 Abs. 1 S. 1, § 9 Abs. 1 S. 1 BVerfSchG; §§ 2 Abs. 1, 5 BNDG; Art. 5 Abs. 1 S. 2, Art. 8 Abs. 1 S. 1 BayVSG; §§ 5 Abs. 1, 5a BWLVSG; § 9 LVerfSchG RP; § 4 Abs. 1, 2, § 5 HVSG; § 5 Abs. 1, 2 VSG NRW; §§ 12 Abs. 1, 14, 15 NVerfSchG; § 7 Abs. 1, § 8 Abs. 1 HmbVerfSchG; § 6 Abs. 1, § 8 BremVerfSchG; § 8 LVerfSchG SH; § 8 VSG Bln; § 6 Abs. 2, 3 BbgVerfSchG; §§ 9, 10 VerfSchG MV; § 7 Abs. 1, 11 Abs. 1 ThürVerfSchG; § 7 Abs. 1, 2, § 8 Abs. 1 VerfSchG-LSA; § 4 Abs. 1, § 5 Abs. 1, 2 SächsVSG; §§ 7 Abs. 1, § 8 Abs. 1 SVerfSchG.

²¹² In Berlin (§ 8 Abs. 2), Brandenburg (§ 6 Abs. 3), Bremen (§ 8), Mecklenburg-Vorpommern (§ 10 Abs. 1), Niedersachsen (§ 14 Abs. 1), Nordrhein-Westfalen (§ 5 Abs. 2), Schleswig-Holstein (§ 8 Abs. 2), vgl. Löffelmann, Hdb. des Rechts der Nachrichtendienste, 1159, 1149 Rn. 77, anders bzgl. des HmbVerfSchG, weil dort auf die abschließende Klärung in einer Dienstvorschrift verwiesen wird, § 8 Abs. 2 S. 2; vgl. auch Löffelmann/Zöller, Nachrichtendienstrecht, S. 101.

²¹³ Kritisch: Siems, NWVbl 2018, 1, 4 f.

²¹⁴ Vgl. auch § 8 Abs. 2 S. 2 BVerfSchG: „In Individualrechte darf nur nach Maßgabe besonderer Befugnisse eingegriffen werden.“

gestützt werden. Als Beispiele für solche Erhebungen lassen sich Recherchen zu bestimmten Personen über Suchmaschinen oder die Auswertung von Zeitungen, Fernsehbeiträgen und Programmen oder Veranstaltungsbesuche anführen.²¹⁵ Die Eingriffsintensität steigt jedoch, wenn diese Maßnahmen systematisch oder automatisiert erfolgen, dann kann eine spezielle Rechtsgrundlage erforderlich sein.²¹⁶

b. Telekommunikationsüberwachung

Alle Nachrichtendienste sind berechtigt, Telekommunikation im Einzelfall, das heißt die Verbindungen bzw. Anschlüsse einer Person, zu überwachen.²¹⁷ Der Begriff der „Telekommunikation“ erfasst die Übermittlung von technischen Signalen über das Internet oder das Telefon.²¹⁸ Eine Telekommunikationsüberwachung (TKÜ) durchzuführen, bedeutet, dass telefonische Gespräche und/oder die Online-Kommunikation durch Mitarbeiter des Nachrichtendienstes unmittelbar zur Kenntnis genommen und gegebenenfalls aufgezeichnet werden.²¹⁹

Die Rechtsgrundlage für die TKÜ im Einzelfall ist für alle Nachrichtendienste einheitlich im G 10 normiert.²²⁰ Im G 10 wird die TKÜ als „Beschränkung im Einzelfall“ bezeichnet (sog. Individualbeschränkung).

c. Quellen-Telekommunikationsüberwachung

Seit 2021 können infolge der Ergänzung des G 10 um § 11 Abs. 1a zudem alle Nachrichtendienste bundesweit eine sog. Quellen-TKÜ durchführen.²²¹ Davor gab es zunächst vereinzelt Rechtsgrundlagen zur Durchführung einer Quellen-TKÜ in Landesverfassungsschutzgesetzen.²²² Mit der Befugnis zur Quellen-TKÜ reagiert der Gesetzgeber darauf, dass viele Internetnutzer heutzutage verschlüsselt miteinander kommunizieren, weshalb die Daten des Kommunikationsvorgangs mit Hilfe der klassischen

²¹⁵ Droste, Verfassungsschutzrecht, S. 227.

²¹⁶ BVerfG 1 BvR 1547/19 - 1 BvR 2634/20 v. 16.2.2023 - Rn. 78, 112.

²¹⁷ Löffelmann, Hdb. des Rechts der Nachrichtendienste, 1159, 1174 Rn. 12.

²¹⁸ § 3 Nr. 59 TKG; Steiner, GSZ 2023, 124, 126.

²¹⁹ Bantlin, JuS 2019, 669, 671.

²²⁰ § 1 Abs. 1 Nr. 1 i. V. m. §§ 3 ff. G 10; Bäcker, Eingriffstatbestände, 137, 143; für diese Norm hat der Bund jedoch keine Gesetzgebungskompetenz vgl. Bäcker, Verfassungsbeschwerde gegen BayVSG, 1, 14 ff.

²²¹ Die damit verbundenen verfassungsrechtlichen Probleme (Normierung als Verfahrensregelung statt Befugnisnorm, Verankerung im G 10, obwohl auch in die Vertraulichkeit und Integrität informationstechnischer Systeme eingegriffen wird) diskutierend: Poscher/Kappler, Verfassungsblog vom 6.7.2021; zustimmend Barczak: „Die Platzierung der Befugnisnorm zwischen Verfahrenserfordernissen wie Antrag, Anordnung und Mitteilung an Betroffene verschleiert den eingriffsintensiven Charakter dieser Neuregelung.“, „(...) zeigt der Gesetzgeber mit der Normierung in § 11 Abs. 1 a G 10, dass er von einem exklusiven Eingriff in das Telekommunikationsgeheimnis ausgeht.“, Barczak, KritV 2021, 91, 123 f.

²²² § 5d BWLVSG; § 8 Abs. 12 HmbVerfSchG

TKÜ nicht mehr abgeschöpft werden können.²²³ Die Quellen-TKÜ umgeht dieses Problem, indem sie mittels einer speziellen Software erlaubt, die Kommunikation bereits an ihrer „Quelle“ anzuzapfen und damit unverschlüsselt auszuleiten, bevor sie verschlüsselt an den eigentlichen Empfänger transportiert wird.²²⁴

d. Online-Durchsuchung

Darüber hinaus ist der bayerische Verfassungsschutz zur Online-Durchsuchung berechtigt.²²⁵ Eine Online-Durchsuchung setzt voraus, dass eine Spähsoftware auf ein elektronisches Gerät aufgespielt wird. Diese ermöglicht es den Behörden, das gesamte informationstechnische System zu durchsuchen.²²⁶ Informationstechnische Systeme, wie beispielsweise PCs, Smartphones, Tablets oder Industriesteueranlagen, „verarbeiten Informationen und Daten“, auf ihnen wird „üblicherweise unterschiedliche Art von Software auf unterschiedlicher Systemebene ausgeführt“, beispielsweise ein Betriebssystem.²²⁷

Die Abgrenzung zwischen Quellen-TKÜ und Online-Durchsuchung ist wegen der vergleichbaren Funktionsweise kompliziert.²²⁸ Zwischen den beiden Maßnahmen besteht jedoch ein grundsätzlicher Unterschied: Während über die Quellen-TKÜ „nur“ Kommunikationsinhalte erfasst werden sollen, ist die Online-Durchsuchung viel weitgehender, weil sie den Zugriff auf alle im Zielsystem gespeicherten Daten ermöglicht.²²⁹

e. Strategische Fernmeldeaufklärung

Davon zu unterscheiden ist die strategische, von Einzelfällen losgelöste, anlasslose Überwachung internationaler Kommunikation, zu der nur der BND ermächtigt ist.²³⁰ Strategische Überwachungen sollen dazu beitragen, Gefahren frühzeitig und unabhängig von verdächtigen Einzelpersonen zu erkennen. Im Rahmen dessen ist der BND befugt, den Telekommunikationsverkehr anlasslos zu sammeln und anhand bestimmter

²²³ „Aufklärungslücke“, BT Drs. 674/20, Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts v. 5.11.2020, S. 22.

²²⁴ Bantlin, JuS 2019, 669, 671; Löffelmann, Hdb. des Rechts der Nachrichtendienste, 1159, 1230 Rn. 104.

²²⁵ Art. 10 Abs. 1 [BayVSG](#).

²²⁶ Bantlin, JuS 2019, 669, 671.

²²⁷ Sobr/Kemmerich, Technische Grundlagen der Informationssicherheit, 49, 52 Rn. 2.

²²⁸ Poscher/Kappler werfen dem Bundesgesetzgeber beispielsweise vor, in § 11 Abs. 1 a G 10 eine „Online-Durchsuchung light“ normiert zu haben, vgl. Poscher/Kappler, Verfassungsblog vom 6.7.2021; Die Quellen-TKÜ als „Sonderform der Online-Durchsuchung“ bezeichnend, Löffelmann, Hdb. des Rechts der Nachrichtendienste, 1283, 1302 Rn. 29.

²²⁹ Ausführlich zur Online-Durchsuchung, Löffelmann, Hdb. des Rechts der Nachrichtendienste, 1283, 1301 ff. Rn. 28 ff.

²³⁰ Bäcker, Eingriffstatbestände, 137, 143; Bantlin, G 10-Kommission, S. 56.

Suchbegriffe (Selektoren) auf relevante Inhalte zu durchforsten.²³¹ Dabei handelt es sich um das „Kerngeschäft“²³² des BND.

Die strategische Überwachung internationaler Telekommunikationsbeziehungen, das heißt solcher Kommunikationen, bei denen sich ein Kommunikationsteilnehmer im Ausland und einer in Deutschland aufhält²³³, ist in § 5 G 10 normiert.²³⁴

Demgegenüber findet man die Normen zur strategischen Überwachung personenbezogener Daten von Ausländern im Ausland (sog. strategische Ausland-Fernmeldeaufklärung) im BNDG, vgl. §§ 19 ff. BNDG. Demnach kann der BND sowohl enorme Mengen an Telekommunikationsverkehrsdaten überwachen (§ 26 Abs. 1 BNDG) als auch gezielt Inhaltsdaten erheben (§ 19 Abs. 1, 4 BNDG). Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 70 TKG) und Informationen über einzelne Kommunikationsverbindungen vermitteln.²³⁵ Mit dem Begriff der Inhaltsdaten sind demgegenüber die Inhalte der Kommunikation gemeint.²³⁶

Für die Aufteilung der rechtlichen Grundlagen in das G 10 einerseits und das BNDG andererseits gibt es keinen sachlichen Grund mehr.²³⁷

f. Eingriffe in informationstechnische Systeme von Ausländern im Ausland

Seit 2021 enthält das BNDG darüber hinaus eine Rechtsgrundlage für Informationserhebungen aus „von Ausländern im Ausland genutzte informationstechnische Systeme[n]“ (§ 34 BNDG).²³⁸ Die Befugnis ist ausweislich der Gesetzesbegründung not-

²³¹ Schenke/Graulich/Ruthig/Huber, § 4 G 10 Rn. 10.

²³² Bantlin, G 10-Kommission, S. 59.

²³³ Bäcker, K&R 2014, 556, 557.

²³⁴ Daneben gibt es eine besondere Form der strategischen Überwachung, falls Personen im Ausland im Einzelfall an Leib und Leben gefährdet sind, vgl. § 8 G 10.

²³⁵ Schenke/Graulich/Ruthig/Mallmann, § 8a BVerfSchG Rn. 12.

²³⁶ Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND/Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 56.

²³⁷ „Insbesondere die Aufspaltung der Befugnisse des BND im G 10 und BNDG ist eine Konsequenz der nunmehr vom Gericht [Anmerkung: vom Bundesverfassungsgericht] als nicht haltbar zurückgewiesenen Auffassung, dass die Grundrechte für die Auslandsaufklärung keine Anwendung finden“, Aust, DöV 2020, 715, 723.

²³⁸ § 34 ff. BNDG, Befugnis zur Online-Durchsuchung von Ausländern im Ausland, die auch ohne den Einsatz von Software möglich ist, wenn sich der Gegenstand im Besitz des BND befindet, § 34 Abs. 9 BNDG.

wendig, weil die strategische Ausland-Fernmeldeüberwachung wegen der zunehmenden Verschlüsselung der Kommunikation mittlerweile weniger ertragreich geworden ist.²³⁹

Der Zugriff auf das IT-System kann mittels einer Überwachungssoftware durchgeführt werden oder analog stattfinden, wenn der BND das IT-System in seinem Besitz hat (§34 Abs. 9 BNDG).²⁴⁰ Nach der erfolgreichen Infiltration des Systems erfolgt die Informationserhebung als Online-Durchsuchung oder Quellen-Telekommunikationsüberwachung.²⁴¹

g. Observationen

Die Befugnis, Observationen durchzuführen, findet man in allen Nachrichtendienstgesetzen.²⁴² Als Observation bezeichnet man die geplante und verdeckte Beobachtung von Personen, Objekten und Ereignissen mit dem Ziel, Informationen zu gewinnen.²⁴³

h. Verdeckte Mitarbeiter und Vertrauensleute

Verdeckte Mitarbeiter und Vertrauensleute sind Personen, die ihre Tätigkeit für den Nachrichtendienst gegenüber den Betroffenen nicht offenlegen. Sie werden dafür eingesetzt, in abgeschotteten, mit anderen nachrichtendienstlichen Mitteln nur schwer erreichbaren Milieus Informationen zu sammeln.²⁴⁴ Verdeckte Mitarbeiter sind Mitarbeiter des Nachrichtendienstes, die gegenüber Dritten unter einer auf Dauer angelegten Legende, das heißt einer zu Tarnungszwecken dauerhaft veränderten Identität²⁴⁵, auftreten. Vertrauensleute hingegen sind Privatleute (aus dem beobachteten Milieu), die dauerhaft mit dem Nachrichtendienst zusammenarbeiten, ohne dass andere Personen Kenntnis davon haben.

²³⁹ Bt-Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 94, vgl. die identische Problematik bei der Telekommunikationsüberwachung [Teil 1 B. III. 1. c.](#)

²⁴⁰ [Steiner](#), GSZ 2023, 124, 126.

²⁴¹ [Dietrich](#), Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12.

²⁴² § 8 Abs. 2 BVerfSchG; § 5 Abs. 2 BNDG, § 8 Abs. 2 BVerfSchG; § 4 Abs. 1 MADG, § 8 Abs. 2 BVerfSchG; Art. 19a, Art. 8 Abs. 1 S. 1 [BayVSG](#); § 5a Abs. 1 [BWLVS](#); über die Generalklausel ohne direkte Nennung § 9 Abs. 1 2 [LVerfSchG RP](#); § 11 [HVSG](#); § 5 Abs. 2 Nr. 2 [VSG NRW](#); § 14 Abs. 1 S. 1 Nr. 7, § 17 [NVerfSchG](#); § 8 Abs. 2 S. 1 Nr. 3 [HmbVerfSchG](#); § 8 Abs. 1 Nr. 3 [BremVerfSchG](#); § 8 Abs. 2 S. 3 Nr. 3 [LVerfSchG SH](#); § 8 Abs. 2 S. 1 Nr. 2 [VSG Bln](#); § 6 Abs. 3 S. 1 Nr. 2, § 10 [BbgVerfSchG](#); § 10 Abs. 1 Nr. 3 [VerfSchG MV](#); § 10 Abs. 1 Nr. 2 [ThürVerfSchG](#); § 7 Abs. 3 S. 1 Nr. 2 [VerfSchG-LSA](#); § 7 Abs. 2 Nr. 5, § 13 [SächsVSG](#); § 8 Abs. 1 S. 2 [SVerfSchG](#).

²⁴³ [Schenke/Graulich/Ruthig/Roth](#), § 8 BVerfSchG Rn. 34.

²⁴⁴ [Dietrich](#), Hdb. des Rechts der Nachrichtendienste, 1017, 1039 Rn. 51.

²⁴⁵ [Dietrich](#), Hdb. des Rechts der Nachrichtendienste, 1017, 1034 Rn. 32.

In der Regel sind die Tatbestandsvoraussetzungen dieser zwei Einsatzmethoden in einer speziellen Ermächtigungsgrundlage normiert.²⁴⁶ Vereinzelt werden sie lediglich als nachrichtendienstliches Mittel aufgezählt.²⁴⁷

Im Saarland und in Sachsen wird der Einsatz Verdeckter Mitarbeiter in keiner Rechtsgrundlage erwähnt, weshalb deren Einsatz dort vermutlich in verfassungswidriger Weise auf die Generalklausel gestützt wird.

i. Verdeckte Ton- und Bildaufzeichnungen (außerhalb oder innerhalb der Wohnung)

Alle Nachrichtendienste sind befugt, das gesprochene Wort aufzunehmen oder Bilder aufzuzeichnen.²⁴⁸ Wenn Gesprächspartner der Zielperson verkabelt oder Mikrofone in Räumlichkeiten versteckt werden, in denen sich der Betroffene außerhalb seiner Wohnung aufhält, handelt es sich dabei um einen Anwendungsfall der Befugnis zur Tonaufzeichnung.²⁴⁹ Bildaufzeichnungen sind demgegenüber manuelle, ferngesteuerte oder automatisierte Video- und Fotoaufnahmen an bestimmten Orten.²⁵⁰

Finden die gleichen Handlungen innerhalb der Wohnung des Betroffenen statt, sind aufgrund der Vorgaben von Art. 13 GG andere, in der Regel detailliertere, Rechtsgrundlagen anwendbar. Die überwiegende Anzahl der Nachrichtendienste sind zu

²⁴⁶ §§ 9a, b BVerfSchG; § 5 BNDG, §§ 9 a, b BVerfSchG; § 5 Abs. 1 Hs. 2 MADG, §§ 9 a, b BVerfSchG; Art. 18, 19 BayVSG; § 6a BWLVSG; §§ 10, 11, 9 2 LVerfSchG RP; §§ 12, 13 HVSG; §§ 5 Abs. 2 Nr. 1, 4 VSG NRW; §§ 16, 18 NVerfSchG; § 8a HmbVerfSchG; § 8 Abs. 1 S. 1 Nr. 1, 2, § 8b BremVerfSchG; § 8 Abs. 2 S. 3 Nr. 1, Abs. 6 LVerfSchG SH; §§ 6a, b BbgVerfSchG; § 10a VerfSchG MV; § 10 Abs. 1 Nr. 1, § 12 ThürVerfSchG; §§ 8 a, b VerfSchG-LSA; § 7 Abs. 2 Nr. 3, 4, § 11, 12 SächsVSG

²⁴⁷ § 8 Abs. 2 S. 1 Nr. 1 VSG Bln; Bzgl. d. Vertrauensleute: § 8 Abs. 1 S. 2 SVerfSchG; zu den Gründen, wieso eine reine Aufzählung dieser Befugnis ohne einen spezifischen Eingriffsanlass nicht verfassungsgemäß sein kann, vgl. *Bäcker*, Eingriffstatbestände, 137, 146.

²⁴⁸ §§ 9 Abs. 1, § 8 Abs. 2 BVerfSchG; § 5 BNDG, § 9 Abs. 1, § 8 Abs. 2 BVerfSchG; § 4 Abs. 1 MADG, § 8 Abs. 2 BVerfSchG; Art. 8 Abs. 1 S. 1 BayVSG; § 5a BWLVSG; § 17 Abs. 1 LVerfSchG RP; § 5 Abs. 1, 2 Nr. 8 HVSG; § 5 Abs. 2 Nr. 3, 6, § 7a VSG NRW; § 14 Abs. 1 S. 1 Nr. 5, § 15 und § 14 Abs. 1 S. 1 Nr. 8, § 17 sowie § 14 Abs. 1 S. 1 Nr. 10, §§ 17, 19 NVerfSchG; § 8 Abs. 2 S. 1 Nr. 4, 7 HmbVerfSchG; § 8 Abs. 1 Nr. 4, 7 BremVerfSchG; § 8 Abs. 2 S. 3 Nr. 2, 4, Abs. 5, 7 LVerfSchG SH; § 8 Abs. 2 S. 1 Nr. 3, 6 VSG Bln; § 6 Abs. 3 S. 1 Nr. 3, 6, § 7 Abs. 3 BbgVerfSchG; § 10 Abs. 1 Nr. 4, 7, Abs. 2-6 VerfSchG MV; § 10 Abs. 1 Nr. 3, 6, Abs. 4 - 8 ThürVerfSchG; §§ 7 Abs. 3 S. 2 Nr. 3, 6, § 8 Abs. 1 VerfSchG-LSA; § 7 Abs. 2 Nr. 10 SächsVSG; § 8 Abs. 1, 2 SVerfSchG.

²⁴⁹ *Löffelmann*, Hdb. des Rechts der Nachrichtendienste, 1159, 1141 Rn. 61.

²⁵⁰ Ebd.

Ton-²⁵¹ und Bildaufzeichnungen²⁵² innerhalb von Wohnungen berechtigt, manche Nachrichtendienstgesetze enthalten jedoch keine solche Rechtsgrundlage^{253 254}.

j. Auskunftsverlangen gegenüber Privatunternehmen

In allen Gesetzen sind Auskunftsverlangen gegenüber privaten Adressaten normiert.

Zunächst können einige Nachrichtendienste Auskunft über Bestandsdaten verlangen: Bei denjenigen, die geschäftsmäßig Telekommunikationsdienste²⁵⁵ erbringen zu Bestandsdaten nach den §§ 3 Nr. 6, 172 bzw. § 174 TKG, und bei denjenigen, die geschäftsmäßig Telemediendienste²⁵⁶ erbringen, zu Bestandsdaten nach § 2 Abs. 2 Nr. 2 TTDSG a.F., das mittlerweile in TDDDG umbenannt wurde.²⁵⁷ Bestandsdaten sind Daten, die sich auf die Vertragsbegründung, die inhaltliche Ausgestaltung, die Änderung und die Beendigung des Vertragsverhältnisses zwischen dem Anbieter und den Nutzern beziehen.²⁵⁸ Dadurch können die Behörden beispielsweise anfragen, wann jemand einen Handyvertrag abgeschlossen hat oder wann ein Facebook-Konto aufgelöst

²⁵¹ § 9 Abs. 2 S. 1, 2 BVerfSchG; § 5 [BNDG](#), §§ 9 Abs. 2 BVerfSchG; § 5 Abs. 1 Hs. 2 MADG, §§ 9 Abs. 2 S. 1, 2 BVerfSchG; Art. 9, 11 [BayVSG](#); § 6 Abs. 1 [BWLVSg](#); § 18 [LVerfSchG RP](#); § 7 [HVSg](#); § 8 Abs. 2 S. 1 Nr. 7, Abs. 3-9, 11 [HmbVerfSchG](#); § 9 [VSG Bln](#); § 11 Abs. 2, 3 [ThürVerfSchG](#); § 8 Abs. 2-5 [VerfSchG-LSA](#); § 7 Abs. 2 Nr. 2, § 9, § 10 [SächsVSG](#); § 8 Abs. 3-6 [SVerfSchG](#).

²⁵² Die Verfassungsschutzbehörde in Thüringen ist nicht zu Bildaufzeichnungen berechtigt.

²⁵³ Die Gesetze in Nordrhein-Westfalen, Niedersachsen, Schleswig-Holstein (§ 8 Abs. 7 S. 2 [LVerfSchG SH](#)), Brandenburg, Mecklenburg-Vorpommern.

²⁵⁴ Offenbar wird von den Normen jedoch kaum Gebrauch gemacht: „Im Bereich des Verfassungsschutzes besitzt die Wohnraumüberwachung aufgrund der engen verfassungsrechtlichen Vorgaben keinerlei praktische Relevanz“, *Löffelmann/Zöller*, Nachrichtendienstrecht, S. 103.

²⁵⁵ Legaldefiniert in § 3 Abs. 1 Nr. 61 TKG: Telekommunikationsdienste sind „gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen: a) Internetzugangsdienste, b) interpersonelle Telekommunikationsdienste und c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden“. Das Augenmerk liegt auf dem technischen Übertragungsvorgang.

²⁵⁶ Vgl. § 1 Abs. 1 TMG (das mittlerweile außer Kraft ist), wonach Telemedien alle elektronischen Informations- und Kommunikationsdienste außer den Telekommunikationsdiensten und dem Rundfunk sind. Hier ist der inhaltliche Aspekt entscheidend (Informationsbereitstellung), nicht der technische Übermittlungsvorgang. Wegen des Erlasses des Digitale-Dienste-Gesetzes müssen die Verweisungen in den Nachrichtendienstgesetzen jedoch überarbeitet werden.

²⁵⁷ § 8d BVerfSchG; § 4 BNDG; § 4b MADG; Art. 14 Abs. 1 [BayVSG](#); § 5c Abs. 1 [BWLVSg](#); § 10 Abs. 1, 3 [HVSg](#); § 7 Abs. 3, § 7c Abs. 1, 2 [HmbVerfSchG](#); § 24b [VerfSchG MV](#); § 17a Abs. 1, Abs. 2 S. 1 Nr. 4 lit.c [VerfSchG-LSA](#); auf die alte Fassung des TKG verweisend: § 13 Abs. 5 [LVerfSchG RP](#); § 5 Abs. 2 Nr. 15 [VSG NRW](#); § 20 Abs. 1 Nr. 1, Abs. 2 Nr. 1, 2 [NVerfSchG](#); § 8a Abs. 1 S. 1 Alt. 2, S. 2 [LVerfSchG SH](#); § 14a Abs. 1, 3 [BbgVerfSchG](#); § 8 Abs. 1, § 9 [ThürVerfSchG](#); bzgl. von TK-Daten: § 8c [BremVerfSchG](#); § 7 Abs. 2 Nr. 8, § 17 Abs. 1 [SächsVSG](#); § 15b [SVerfSchG](#). Das [VSG Bln](#) enthält keine vergleichbare Rechtsgrundlage.

²⁵⁸ Vgl. § 2 Abs. 2 Nr. 2 TTDSG; *Gärditz*, Hdb. des Rechts der Nachrichtendienste, 967, 984 Rn. 23.

wurde. Bei ersterem handelt es sich um Bestandsdaten zu einem Telekommunikationsvertrag, bei zweiterem um solche eines Telemedienvetrags. Die in den Nachrichtendienstgesetzen normierten Rechtsgrundlagen sind im Sinne des Doppeltür-Modells diejenigen Normen, die den Nachrichtendiensten die Abfrage erlauben („Abfragetür“ in Abgrenzung zur Übermittlungsermächtigung des Privaten).²⁵⁹

Darüber hinaus können bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, Verkehrsdaten eingeholt werden.²⁶⁰ Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 70 TKG). Im Gegensatz zu den Bestandsdaten, die sich auf das Vertragsverhältnis beziehen, vermitteln Verkehrsdaten Informationen über einzelne Kommunikationsverbindungen.²⁶¹

Darüber hinaus existieren in den Nachrichtendienstgesetzen Normen, auf deren Grundlage bei Tele(medien)anbietern²⁶² Nutzungsdaten abgefragt werden dürfen. Es handelt sich dabei um Daten, „deren Verarbeitung erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen“, insbesondere Daten zur Identifikation des Nutzers, den jeweiligen Nutzungsvorgängen und den in Anspruch genommenen Telemedien (§ 2 Abs. 2 Nr. 3 TTDSG).²⁶³

²⁵⁹ Schenke/Graulich/Ruthig/*Graulich*, § 8d BVerfSchG Rn. 1; zum Doppeltürmodell beispielsweise BVerfG, Beschluss v. 27.5.2020, 1 BvR 1873/13 - 1 BvR 2618/13 – Rn. 93.

²⁶⁰ Einholung von Verkehrsdaten i.S. v. § 9 Abs. 1 S. 1 TTDSG; § 8a Abs. 1 Nr. 4 BVerfSchG; § 3 BNDG; § 8a Abs. 1 S. 1 Nr. 4 BVerfSchG; § 4a MADG; § 8a Abs. 1 Nr. 4 BVerfSchG; Art. 15 Abs. 2 Nr. 2 BayVSG; § 5b Abs. 3 BWLVSG; § 10 Abs. 4 Nr. 2 HVSG; § 7c Abs. 2 VSG NRW; § 7 Abs. 3 S. 1 Nr. 4 HmbVerfSchG; § 27a Abs. 4 VSG Bln; § 24a Abs. 1 S. 1 Nr. 4 VerfSchG MV; § 17a Abs. 2 S. 1 Nr. 4 lit.a VerfSchG-LSA; § 7 Abs. 2 Nr. 7, § 15 Abs. 1 S. 1 Nr. 3 SächsVSG; auf die alte Fassung verweisend: § 13 Abs. 4 LVerfSchG RP; § 20 Abs. 2 S. 1 Nr. 3 NVerfSchG; § 8a Abs. 2 S. 1 Nr. 4 LVerfSchG SH; § 14a Abs. 4 Nr. 2 BbgVerfSchG; § 8 Abs. 2 S. 1 Nr. 3 ThürVerfSchG. Das SVerfSchG und das BremVerfSchG enthalten keine vergleichbaren Rechtsgrundlagen. § 8b Abs. 10 BVerfSchG, der den Landesgesetzgeber eine vergleichbare Regelung nur unter Wahrung gewisser Voraussetzung gestattet, ist kompetenzwidrig, weil sich die Gesetzgebungskompetenz des Bundes auf die Regelung der „Zusammenarbeit“ beschränkt (vgl. [Teil 1 B. I. 1](#)), *Gärditz*, Hdb. des Rechts der Nachrichtendienste, 967, 1007 Rn. 71.

²⁶¹ Schenke/Graulich/Ruthig/*Mallmann*, § 8a BVerfSchG Rn. 12.

²⁶² Zum Unterschied der Begriffe Telemedienanbieter und Teleanbieter: Schenke/Graulich/Ruthig/*Mallmann*, § 8a BVerfSchG Rn. 4a.

²⁶³ § 8a Abs. 1 Nr. 5 BVerfSchG; § 3 BNDG; § 8a Abs. 1 Nr. 5 BVerfSchG; § 4a MADG; § 8a Abs. 1 Nr. 5 BVerfSchG; Art. 15 Abs. 2 Nr. 3 BayVSG; § 5b Abs. 3 BWLVSG; § 10 Abs. 4 Nr. 3 HVSG; § 7c Abs. 2 VSG NRW; § 7 Abs. 3 S. 1 Nr. 5 HmbVerfSchG; § 8a Abs. 2 S. 1 Nr. 5 LVerfSchG SH; § 27a Abs. 4 VSG Bln; § 14a Abs. 4 Nr. 3 BbgVerfSchG; § 24a Abs. 1 Nr. 5 VerfSchG MV; § 8 Abs. 2 S. 1 Nr. 4 ThürVerfSchG; § 17a Abs. 2 S. 1 Nr. 5 VerfSchG-LSA; § 7 Abs. 2 Nr. 7, § 15 Abs. 1 S. 1 Nr. 4 SächsVSG; auf die alte Rechtsgrundlage verweisend: § 13 Abs. 4 LVerfSchG RP; § 20 Abs. 1 S. 1 Nr. 2 NVerfSchG. Das SVerfSchG und das BremVerfSchG enthalten keine vergleichbaren Rechtsgrundlagen.

Gegenüber Flugunternehmen, Computerreservierungs- und Distributionsunternehmen können die Nachrichtendienste erfragen, wer wann welche Flüge wahrgenommen hat und auf welchem Weg diese Flüge gebucht wurden.²⁶⁴ Dadurch sollen die Nachrichtendienste befähigt werden, Bewegungsprofile von Terroristen zu erstellen und denkbare Angriffsziele zu erkennen.²⁶⁵

Um einen Einblick in Geldflüsse und Kontobewegungen von beobachteten Personengruppen zu erlangen, sind die Nachrichtendienste gesetzlich dazu ermächtigt, bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen Kontodaten abzufragen.²⁶⁶ So können Kontoinhaber identifiziert oder Überweisungen nachverfolgt werden.²⁶⁷ Teilweise können die Nachrichtendienstbehörden über das Bundeszentralamt für Steuern Kontostammdaten abrufen.²⁶⁸ Es handelt sich dabei um Informationen über das Vertragsverhältnis, die von beteiligten Kreditinstituten erhoben werden.²⁶⁹

In einigen Gesetzen ist vorgesehen, dass die Nachrichtendienste bei Postdienstleistern Auskünfte zu Umständen des Postverkehrs einholen können, hierunter fallen beispielsweise Name und Anschrift des Versenders oder Empfängers.²⁷⁰

²⁶⁴ § 8a Abs. 1 Nr. 1 BVerfSchG; § 3 BNDG, § 8a Abs. 1 Nr. 1 BVerfSchG; § 4a MADG, § 8a Abs. 1 Nr. 1 BVerfSchG; Art. 16 Abs. 1 Nr. 1 [BayVSG](#); § 5b Abs. 1 Nr. 2 [BWLVS](#)G; zu jeglichen „Transportleistungen“ gem. § 13 Abs. 2 [LVerfSchG RP](#), § 14a Abs. 2 S. 1 Nr. 1 [BbgVerfSchG](#); § 10 Abs. 2 S. 1 Nr. 1 [HVSG](#); § 20 Abs. 3 S. 1 Nr. 1 [NVerfSchG](#); § 7 Abs. 3 S. 1 Nr. 1 [HmbVerfSchG](#); § 8a Abs. 2 Nr. 1 [LVerfSchG SH](#); § 27a Abs. 3 [VSG Bln](#); § 24a Abs. 1 Nr. 1 [VerfSchG MV](#); § 8 Abs. 2 S. 1 Nr. 1 [ThürVerfSchG](#); § 17a Abs. 2 S. 1 Nr. 1 [VerfSchG-LSA](#); § 7 Abs. 2 Nr. 7, § 15 Abs. 1 S. 1 Nr. 2 [SächsVSG](#). Das [VSG NRW](#), das [SVerfSchG](#) und das [BremVerfSchG](#) enthalten keine vergleichbaren Rechtsgrundlagen.

²⁶⁵ Schenke/Graulich/Ruthig/*Mallmann*, § 8a BVerfSchG Rn. 9; *Droste*, Verfassungsschutzrecht, S. 241.

²⁶⁶ § 8a Abs. 1 Nr. 2 BVerfSchG; § 3 BNDG, § 8a Abs. 1 Nr. 2 BVerfSchG; § 4a MADG, § 8a Abs. 1 Nr. 2 BVerfSchG; Art. 16 Abs. 1 Nr. 2 [BayVSG](#); § 5b Abs. 1 Nr. 1 [BWLVS](#)G; § 13 Abs. 1 S. 1 [LVerfSchG RP](#); § 10 Abs. 2 S. 1 Nr. 2 [HVSG](#); § 7c Abs. 1 [VSG NRW](#); § 20 Abs. 3 S. 1 Nr. 2 [NVerfSchG](#); § 7 Abs. 3 S. 1 Nr. 2 [HmbVerfSchG](#); § 8a Abs. 2 S. 1 Nr. 2 [LVerfSchG SH](#); § 27a Abs. 1 [VSG Bln](#); § 14a Abs. 2 S. 1 Nr. 2 [BbgVerfSchG](#); § 24a Abs. 1 Nr. 2 [VerfSchG MV](#); § 8 Abs. 2 S. 1 Nr. 2 [ThürVerfSchG](#); § 17a Abs. 2 S. 1 Nr. 2 [VerfSchG-LSA](#); § 7 Abs. 2 Nr. 7, § 15 Abs. 1 S. 1 Nr. 1 [SächsVSG](#). Das [SVerfSchG](#) und das [BremVerfSchG](#) enthalten keine vergleichbaren Rechtsgrundlagen.

²⁶⁷ Schenke/Graulich/Ruthig/*Mallmann*, § 8a BVerfSchG Rn. 11.

²⁶⁸ § 8a Abs. 2 BVerfSchG; § 3 [BNDG](#), § 8a Abs. 2 BVerfSchG; § 4a [MADG](#), § 8a Abs. 2 BVerfSchG; Art. 16 Abs. 2 [BayVSG](#); § 5c Abs. 3 [BWLVS](#)G; § 13 Abs. 1 S. 2 [LVerfSchG RP](#); § 20 Abs. 4 [NVerfSchG](#); § 7 Abs. 4 [HmbVerfSchG](#); § 17a Abs. 2a [VerfSchG LSA](#); § 7 Abs. 2 Nr. 9, § 17 Abs. 6 [SächsVSG](#); die Befugnis des Bundeszentralregisters an die Länderbehörden zu übermitteln, ergibt sich aus § 93b Abs. 2, § 93 Abs. 8 S. 1 Nr. 3 AO.

²⁶⁹ Schenke/Graulich/Ruthig/*Mallmann*, § 8a BVerfSchG Rn. 20.

²⁷⁰ Art. 15 Abs. 2 Nr. 1 [BayVSG](#); § 5b Abs. 2 [BWLVS](#)G; § 13 Abs. 3 [LVerfSchG RP](#); § 10 Abs. 1 [HVSG](#); § 5 Abs. 2 Nr. 10 [VSG NRW](#); § 8a Abs. 1, 2 S. 1 Nr. 3 [LVerfSchG SH](#); § 27a Abs. 2 [VSG Bln](#); § 14a Abs. 1 [BbgVerfSchG](#); § 24a Abs. 2 Nr. 3 [VerfSchG MV](#); § 17a Abs. 2 S. 1 Nr. 3 [VerfSchG LSA](#).

k. Verdeckte Erhebung von Daten aus Sozialen Medien

Mehrere Gesetzgeber haben überdies eine Rechtsgrundlage für die (verdeckte) Erhebung von Daten unter Ausnutzung eines berechtigten Vertrauens aus öffentlich zugänglichen Sozialen Medien geschaffen.²⁷¹ Wenn die Behörde unter dem Namen eines Kommunikationspartners oder einer sonst berechtigten Person tätig wird oder sie sogar verdeckt auf zugangsgesicherte Inhalte in Sozialen Medien zugreift und dadurch ein schutzwürdiges Vertrauen in die Identität des Gegenübers besteht, liegt darin ein Eingriff in das Recht auf Informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.²⁷² Für diese Eingriffe sollen die neu geschaffenen Normen als Rechtsgrundlage dienen.

l. IMSI/IMEI Catcher

Einige Fachgesetze ermöglichen die Identifizierung und Lokalisierung von mobilen Telekommunikations-Endgeräten unter Einsatz des sog. IMSI/IMEI (International Mobile Subscriber Identity)-Catcher.²⁷³ Beim IMSI/IMEI-Catcher handelt es sich um ein technisches Gerät, mit dem eine Funkzelle simuliert werden kann, um auf diese Weise die SIM-Kartennummer (International Mobile Subscriber Identity) oder Gerätekennummer (International Mobile Equipment Identity) von Mobiltelefonen identifizieren zu können.²⁷⁴ Die Maßnahme dient der Standortbestimmung des Geräts oder der Vorbereitung von Telekommunikationsüberwachungen und Observationen in Situationen, bei denen die Behörde keine Informationen darüber hat, welches Handy die beobachtete Person nutzt und deshalb ein Auskunftsverlangen gegenüber Telekommunikationsunternehmen erfolglos wäre.²⁷⁵ Der Standortbestimmung dient auch die in einem Landesverfassungsschutzgesetz normierte Funkzellenabfrage, bei der die Behörden sich bei Telekommunikationsanbietern darüber informieren, welche Geräte

²⁷¹ § 20 [LVerfSchG RP](#); § 5 Abs. 2 Nr. 11 [HVSG](#); § 5 Abs. 2 Nr. 11, § 7a [VSG NRW](#); § 14 Abs. 1 Nr. 3, § 15 [NVerfSchG](#); § 8 Abs. 2 S. 2 Nr. 4 [LVerfSchG SH](#); § 10 Abs. 1 Nr. 12 [VerfSchG MV](#); § 7 Abs. 3 S. 2 Nr. 10 [VerfSchG LSA](#); § 7 Abs. 2 Nr. 13, § 11 Abs. 7 [SächsVSG](#); die Norm über Verdeckte Mitarbeiter entsprechend anwendend: Art. 18 Abs. 5 [BayVSG](#); § 6 Abs. 3 S. 1 Nr. 12 [BbgVerfSchG](#).

²⁷² BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 310.

²⁷³ § 9 Abs. 4 BVerfSchG; § 5 BNDG; § 9 Abs. 4 BVerfSchG; § 5 MADG; § 9 Abs. 4 BVerfSchG; § 6 Abs. 2 [BWLVS](#); § 15 Abs. 1 [LVerfSchG RP](#); § 9 [HVSG](#); § 7b [VSG NRW](#); § 14 Abs. 1 Nr. 11, §§ 15, 19 [NVerfSchG](#); § 8 Abs. 10 [HambVerfSchG](#); § 8 Abs. 2 S. 2 Nr. 6 [LVerfSchG SH](#); § 6 Abs. 3 Nr. 11 [BbgVerfSchG](#); § 10 Abs. 7 [VerfSchG MV](#); § 10 Abs. 1 Nr. 11 [ThürVerfSchG](#); § 17a Abs. 6 [VerfSchG-LSA](#); § 8 Abs. 7 [SVerfSchG](#); § 7 Abs. 2 Nr. 6, § 14 [SächsVSG](#); zur „punktuellen Ermittlung des Standorts eines aktiv geschalteten Mobilfunkendgeräts“: Art. 12 Abs. 1, 19a [BayVSG](#).

²⁷⁴ Genaue Beschreibung der Funktionsweise: [Löffelmann](#), Hdb. des Rechts der Nachrichtendienste, 1283, 1325 Rn. 67.

²⁷⁵ Schenke/Graulich/Ruthig/[Mallmann](#), § 9 BVerfSchG Rn. 36; [Löffelmann](#), Hdb. des Rechts der Nachrichtendienste, 1283, 1325 Rn. 67.

sich zu einem bestimmten Zeitpunkt in einer Funkzelle befanden (§ 14 LVerfSchG RP).²⁷⁶

m. Sonstige Befugnisse

Vereinzelte wird den Nachrichtendiensten überdies eine vorübergehende Inbesitznahme von Sachen zur heimlichen Datenerhebung (§ 16 LVerfSchG RP) sowie der Zugriff auf Videoüberwachung des öffentlich zugänglichen Raums ermöglicht, auch in Echtzeit (§ 21 LVerfSchG RP).

n. Auswertung und Übermittlung

Die von den Nachrichtendiensten mit den beschriebenen Mitteln erhobenen Informationen werden gespeichert und regelmäßig an andere öffentliche oder private Stellen übermittelt, weshalb alle Fachgesetze spezielle Übermittlungsnormen enthalten. Nach der Erhebung werden die Daten in Akten oder Dateien gespeichert, sortiert und ausgewertet, um themenspezifisch informieren zu können.²⁷⁷ Fast alle Fachgesetze enthalten eine Rechtsgrundlage zur Speicherung, Veränderung und Nutzung personenbezogener Daten.²⁷⁸

2. Keine abschließende Normierung

Nur wenn es für eine nachrichtendienstliche Tätigkeit eine solche (spezifische) gesetzliche Grundlage gibt, kann die Rechtmäßigkeit kontrolliert werden. Der Gesetzgeber müsste deshalb bemüht sein, für alle Tätigkeiten der Nachrichtendienste, die in Grundrechte eingreifen, eine gesetzliche Grundlage zu schaffen.²⁷⁹ Es gibt jedoch Anhaltspunkte dafür, dass dies nicht vollständig der Fall ist.

So weist *Barczak* darauf hin, dass es für die Tätigkeit des BfV im Ausland de lege lata keine Ermächtigung gibt.²⁸⁰ Auch die Tätigkeit des BND im Ausland wird von den

²⁷⁶ *Löffelmann*, Hdb. des Rechts der Nachrichtendienste, 1283, 1326 Rn. 68.

²⁷⁷ *Warg*, Hdb. des Rechts der Nachrichtendienste, 509, 513 Rn. 1.

²⁷⁸ § 10 BVerfSchG; § 6 BNDG; § 6 MADG; Umkehrschluss aus Art. 21 [BayVSG](#); § 7 [BWLVS](#); § 23 [LVerfSchG RP](#); § 16 [HVS](#); § 8 [VSG NRW](#); § 26 [NVerfSchG](#); § 9 [HmbVerfSchG](#); § 6 Abs. 1, § 11 [BremVerfSchG](#); §§ 11 ff. [LVerfSchG SH](#); § 11 [VSG Bln](#); § 8 [BbgVerfSchG](#); § 15 [VerfSchG MV](#); § 13 [ThürVerfSchG](#); § 9 [VerfSchG-LSA](#); § 18 [SächsVSG](#); § 10 [SVerfSchG](#).

²⁷⁹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 Rn. 201; bezeichnet die abschließende Aufzählung der nachrichtendienstlichen Mittel zutreffend bereits 1981 als „rechtstaatlich ‚sauberste‘ Lösung“, *Bull.*, Datenschutz, 133, 146.

²⁸⁰ *Barczak*, Nachrichtendienstliche Beobachtung, 193, 213.

aktuellen Rechtsgrundlagen nicht erfasst, vgl. § 1 Abs. 2 S. 2 BNDG. Für das Militärische Nachrichtenwesen gibt es keine Rechtsgrundlagen.²⁸¹ *Wetzling/Vieth* führen aus, dass es für den Dateneinkauf von privaten Unternehmen keine Rechtsgrundlage gibt²⁸², soweit er tatsächlich erfolgt, was nur Insider bewerten können. Zudem ist die Gewinnung von Erkenntnissen durch menschliche Quellen („HUMINT“) – vom Einsatz Verdeckter Mitarbeiter und von Vertrauensleuten abgesehen – gesetzlich nicht speziell geregelt.²⁸³ De lege lata wird hierfür auf die Generalklauseln zurückgegriffen.²⁸⁴

Solange keine speziellen Rechtsgrundlagen geschaffen sind, müssen den Kontrolleuren zumindest die internen Verwaltungsvorschriften vorgelegt werden²⁸⁵, mit denen die Praxis der Nachrichtendienstmitarbeiter angeleitet wird.

Unabhängig von Überlegungen zur Kontrollierbarkeit muss jedoch schon aus Gründen der Transparenz öffentlich erkennbar sein, über welche geheime Befugnisse die Nachrichtendienste verfügen. Das Geheimhaltungsbedürfnis der Nachrichtendienste kann sich im demokratischen Rechtsstaat nicht „auf die Rahmenbedingungen der Aufgabenwahrnehmung“ erstrecken.²⁸⁶ Deshalb ist eine „systematische Neuordnung“ der Nachrichtendienstgesetze „anzustreben, die als vollständige Kompetenzgesetze alle Befugnisse des jeweiligen Nachrichtendienstes normenklar in einem Gesetz nach dem Vorbild des BKA-Gesetzes abbilden sollten (...)“.²⁸⁷

3. Tatbestandliche Weite der Befugnisnormen

Die Tatbestandsvoraussetzungen der Befugnisnormen im Detail miteinander zu vergleichen, würde wegen der erheblichen Unterschiede in der Ausgestaltung den Umfang dieser Untersuchung sprengen. Unabhängig von der Ausgestaltung im Detail lässt sich jedoch feststellen, dass die Normen überwiegend weit formuliert sind. Die Rechtsgrundlagen für den Einsatz nachrichtendienstlicher Mittel gemäß dem BVerfSchG, auf die sowohl das MADG als auch das BNDG verweisen, sind in der Regel so weit gefasst,

²⁸¹ *Huber*, NVwZ-Beilage 2021, 3, 8; *Sosna*, GSZ 2022, 245, 247; *Wetzling/Ruckerbauer*, Zügellose Überwachung?, S. 22 ff.; *BfDI*, Das Militärische Nachrichtenwesen 2023.

²⁸² *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 9; Weil die Kontrolleure sich auf ihren gesetzlich normierten Aufgabenkatalog konzentrieren, werden solche noch nicht normativ gestützten Praktiken vermutlich nicht untersucht, *Wetzling/Dietrich*, Disproportionate use of commercially and publicly available data, S. 40.

²⁸³ BT-Drs. 19/26221, Antrag B 90/Die Grünen v. 27.1.2021, S. 7.

²⁸⁴ §§ 9 Abs. 1, 8 Abs. 2 BVerfSchG, § 5 BNDG bzw. § 5 MADG, § 9 Abs. 1, § 8 Abs. 2 BVerfSchG.

²⁸⁵ Fordert, dass „bis zu einer gesetzlichen Regelung“ durch „Verwaltungsvorschriften (Richtlinien) ein höheres Maß an Klarheit geschaffen“ werden sollte, *Bull*, Datenschutz 1981, 133, 147.

²⁸⁶ *Masing*, Nachrichtendienste, 3, 13; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 201.

²⁸⁷ *Bartodziej*, Hdb. des Rechts der Nachrichtendienste, 1533, 1606 Rn. 135; insoweit entfaltet das novellierte Sächsische Verfassungsschutzgesetz eine Vorbildfunktion, weil § 7 [SächsVSG](#) alle nachrichtendienstlichen Mittel abschließend aufzählt, Entwurf eines Gesetzes zur Neuregelung des Nachrichtendienstrechts, Drs. 7/15464 v. 11.01.2024, S. 5.

dass „sie in erheblichem Ausmaß die verfassungsrechtlichen Anforderungen hinsichtlich Eingriffsschwellen und verfahrensrechtlicher Sicherungen verfehlen“²⁸⁸, was für die Landesverfassungsschutzgesetze gleichermaßen gilt.

a. Beispiele für weite Regelungen

Besonders weit sind Regelungstechniken, die die zulässigen nachrichtendienstlichen Mittel nicht enumerativ benennen, sondern auf eine Aufzählung in Dienstvorschriften verweisen oder sich vorbehalten, zusätzliche nachrichtendienstliche Mittel in solchen Dienstvorschriften zu regeln.²⁸⁹ Eine Konsequenz dieser Regulationsweise ist, dass Dritte, die keinen Zugang zu diesen Dienstvorschriften haben, nicht wissen können, welche nachrichtendienstlichen Mittel von der Behörde eingesetzt werden dürfen.

Typischerweise enthält die Befugnisnorm keine Begrenzung der Adressaten, sodass nicht nach Verantwortlichkeitsgraden differenziert wird. Überwiegend ist es für ihre Anwendung schon ausreichend, wenn ein Bezug zu einer Bestrebung hergestellt werden kann.²⁹⁰ Gegen wen sie eingesetzt werden dürfen, ergibt sich aus ihnen nicht.²⁹¹

Sehr unscharf sind darüber hinaus diejenigen Eingriffsermächtigungen, die an eine „Gefahr“ für ein Schutzgut des Nachrichtendienstes anknüpfen. Wann eine Gefahr im nachrichtendienstlichen Sinn vorliegt, wird nicht detailliert. Auf den polizeirechtlichen Gefahrbegriff kann jedenfalls – außer für die Wohnraumüberwachungen und Online-Durchsuchungen²⁹² – nicht zurückgegriffen werden, weil der Nachrichtendienst im Vorfeld einer polizeilichen Gefahr tätig wird.²⁹³

²⁸⁸ Barczak, KritV 2021, 91, 131.

²⁸⁹ Art. 8 Abs. 2 BayVSG; § 5a BWLVSG; § 9 Abs. 2 S. 2 LVerfSchG RP; § 8 Abs. 2 S. 2 HmbVerfSchG; § 8 Abs. 1 S. 2 SVerfSchG.

²⁹⁰ Anders beispielsweise § 18 Abs. 3 S. 2 LVerfSchG RP, der Wohnraumüberwachungen Dritter normiert.

²⁹¹ Zu Art. 5, Art. 8 BayVSG: Bäcker, Beschwerdeschrift G 10, S. 29, 30; Gusy, VerwArch 2015, 437, 453; Barczak führt aus, dass die polizeirechtlichen Verantwortlichkeitsnormen zwar nicht übertragbar sind, es aus rechtsstaatlichen Gründen jedoch erforderlich wäre, einen „nachrichtendienstlichen Störerbegriff“ zu entwickeln, Barczak, KritV 2021, 91, 110; Lindner/Unterreitmeier, DöV 2019, 165, 173.

²⁹² Diese Maßnahmen sind so eingriffsintensiv, dass mindestens eine konkrete oder konkretisierte Gefahr im polizeirechtlichen Sinn vorliegen muss, vgl. BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 158, 163 ff., 181.

²⁹³ Vgl. Teil 1 B. II. 2. a, sowie im Detail: Bäcker, Beschwerdeschrift G 10, S. 32 ff., 41 f.; u.a. BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 163, 329: „Diese polizeiliche Gefahrenschwelle würde im Tätigkeitsbereich des Landesamts für Verfassungsschutz, wie die Beschwerdeführer zutreffend ausführen, kaum je erreicht. Der Gesetzgeber wollte hier aber zweifellos keine für den Verfassungsschutz nahezu prohibitive Schwelle errichten.“

b. Vorgaben aus der Entscheidung zum Bayerischen Verfassungsschutzgesetz

In seiner Entscheidung aus dem April 2022²⁹⁴ hat das Bundesverfassungsgericht die Anforderungen für eine verfassungskonforme Ausgestaltung nachrichtendienstlicher Befugnisse weiter herausgearbeitet. Die darin formulierten Grundsätze für die Tatbestandsgestaltung werden nur überblicksartig dargestellt.

Demnach gelten für sehr eingriffsintensive nachrichtendienstlichen Befugnisse, die eine weitgehende Erfassung der Persönlichkeit ermöglichen, dieselben strengen Vorgaben wie für polizeiliche Maßnahmen. Deshalb können Befugnisse wie die Wohnraumüberwachung oder Online-Durchsuchungen nur angewandt werden, wenn eine hinreichend konkretisierte Gefahr vorliegt.²⁹⁵

Bei weniger eingriffsintensiven Maßnahmen ist keine konkretisierte Gefahr notwendig. Allerdings muss dann ein hinreichender verfassungsschutzspezifischer Aufklärungsbedarf bestehen. Dieser wird bejaht, wenn eine Maßnahme zur Aufklärung einer „bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten“ ist und „auf hinreichenden tatsächlichen Anhaltspunkten“ beruht. Je höher das Eingriffsgewicht der Maßnahme ist, umso dringender muss die „Überwachungsbedürftigkeit“ sein. Wenn Unbeteiligte von den Maßnahmen erfasst werden, gelten besondere Anforderungen. Für eingriffsintensive Maßnahmen muss eine unabhängige Vorabkontrolle eingerichtet werden.²⁹⁶

Das Bundesverfassungsgericht hat auch Aussagen über den Adressaten einer nachrichtendienstlichen Befugnis getroffen. Demnach müssen jedenfalls in den Verfassungsschutzgesetzen bestimmte Stufen der Beobachtungsbedürftigkeit einer Bestrebung differenziert werden, die im Gesetz abstrakt abzubilden sind: je eingriffsintensiver die Maßnahme, desto beobachtungsbedürftiger muss die Bestrebung sein.²⁹⁷

Die Praxis, nachrichtendienstliche Befugnisse nur in Dienstvorschriften zu regeln, ist mit der neuesten Rechtsprechung nicht vereinbar. Das Bundesverfassungsgericht hat klargestellt, dass die Befugnisse der Nachrichtendienste „durch Gesetz normenklar und bestimmt vor der Öffentlichkeit geregelt“ sein müssen, denn „[f]ür die Handlungsgrundlagen und Grenzen ihrer Befugnisse kann es im demokratischen Rechtsstaat eine prinzipielle Geheimhaltung nicht geben“.²⁹⁸

Diese Vorgaben sind auf die anderen Nachrichtendienstgesetze übertragbar. Damit steht fest, dass die Befugnisnormen zukünftig wesentlich detaillierter formuliert sein

²⁹⁴ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17.

²⁹⁵ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 175 ff.; Gärditz, GSZ 2022, 161, 162.

²⁹⁶ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 181.

²⁹⁷ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 184 ff., 202 ff.

²⁹⁸ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 201.

müssen. Dass die tradierte, extrem weite Regelungsweise nicht verfassungskonform ist, ist spätestens seit dem Grundsatzurteil aus dem April 2022 offensichtlich.

c. Gründe für die tatbestandliche Weite

Dafür, dass die Befugnisnormen im Nachrichtendienstrecht bisher sehr weitmaschig formuliert sind, gibt es unterschiedliche Begründungen.

Zum einen wird mit dem Vorfeldcharakter nachrichtendienstlicher Tätigkeit argumentiert. Da der nachrichtendienstliche Auftrag vorrangig darin bestehe, den politischen Entscheidungsträgern Informationen zur Gefahrenfrüherkennung zu übermitteln, den Nachrichtendiensten jedoch keine imperativen Befugnisse zur Verfügung stünden, sei eine weitmaschige Regelungsgrundlage unschädlich. Im Vergleich zur Arbeit der Polizei- und Strafverfolgungsbehörden sei die Tätigkeit der Nachrichtendienste für die Betroffenen weniger risikoreich.²⁹⁹

Dieses Argument setzt voraus, dass die Übermittlung von Nachrichtendiensten an andere Sicherheitsbehörden rechtlich an hohe Voraussetzungen gebunden sind, die in der Praxis tatsächlich eingehalten werden. Andernfalls ist die Tätigkeit der Nachrichtendienste für die Betroffenen auch nicht weniger risikoreich als die der anderen Sicherheitsbehörden. Außerdem ergibt sich aus der Entscheidung zum Bayerischen Verfassungsschutzgesetz, dass das Bundesverfassungsgericht die Befugnisnormen als nicht präzise genug erachtet und insoweit erheblicher Nachsteuerungsbedarf besteht. In Bezug auf die aktuelle Rechtslage überzeugt diese Argumentation daher nicht.

Darüber hinaus wird als Argument gegen eine präzise Ausgestaltung der Befugnisnormen darauf verwiesen, dass eine zu detaillierte Ausgestaltung denjenigen einen Vorteil verschaffen würde, die man zu beobachten versucht: Auf diese Weise ermögliche man es diesen Personen, einer Beobachtung zu entgehen.³⁰⁰ Zu Recht wird dagegen eingewandt, dass solche Konsequenzen in den anderen Bereichen des Sicherheitsrechts offensichtlich nicht gefürchtet werden.³⁰¹

Ein zusätzlicher Grund für die Weite der Befugnisnormen ist, dass sehr weite Normen den Handlungsspielraum der Praxis erhöhen und damit im Interesse der Nachrichtendienste sind.

Dass die Rechtsgrundlagen der Nachrichtendienste (teilweise) weitmaschig formuliert waren bzw. sind, ist kein Spezifikum des deutschen Nachrichtendienstrechts, sondern tritt auch anderswo auf:

²⁹⁹ *Bäcker*, Eingriffstatbestände, 137, 144; vgl. auch BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 156 ff.

³⁰⁰ Diese Haltung beschreibend *Gusy*, VerwArch 2015, 437, 438.

³⁰¹ *Gusy*, VerwArch 2015, 437, 438 f.

*„The exploitation of legal ambiguity appears to have been a central feature of state surveillance that allowed it to grow in size and complexity to the extent exposed by Snowden. Although some of this may have been attributable to rapid technological development outstripping dated legal foundations, it was also the case that until recently (and in many countries still) the legislation specifying the powers of the agencies was **vague by design**. Such laws were intended to give a cloak of legitimacy – sufficient to satisfy the criteria of being ‘in accordance with the law’ – but without drawing undue attention to the mechanics, capabilities (and limitations) of surveillance.“³⁰²*

Häufig steht dahinter – bedauerlicherweise auch in Rechtsstaaten – demnach die Motivation, die Tätigkeit der Nachrichtendienste nach außen hin möglichst im Vagen zu lassen.

4. Schlüsselfaktor für die Kontrolltiefe

Für die Kontrolle der Nachrichtendienste sind diese Überlegungen zur Ausgestaltung der Befugnisnormen deshalb relevant, weil es sich dabei (im Zusammenspiel mit den Auftragsnormen) zugleich um die Verhaltensnormen der Nachrichtendienste handelt.³⁰³

Die Kontrolltiefe, ein maßgeblicher Faktor für die Bewertung von Kontrolle, ist unter anderem davon abhängig, wie detailliert das zu kontrollierende Verhalten in den Verhaltensnormen vorgegeben ist.³⁰⁴ Gusy stellt dazu fest, dass eine entscheidende Voraussetzung für das Gelingen von Kontrolle darin besteht, dass „das maßgebliche Recht hinreichende Kriterien für die Abgrenzung von rechtmäßigem bzw. rechtswidrigem Handeln enthält“. ³⁰⁵ Die Kontrolle sei zunehmend schlechter umsetzbar, je weiter diese Kriterien gefasst werden. Sich explizit auf die Nachrichtendienstgesetze beziehend, führt er fort:

³⁰² Leigh/Wegge, Oversight, 7, 15 f.

³⁰³ Vgl. zum Begriff der Verhaltensnorm [Teil 1 A. II. 6.](#)

³⁰⁴ Vgl. [Teil 1 A. II. 8.](#); so auch BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 258: „Sie [die richterliche Vorabkontrolle] ist zwar nicht dazu geeignet, die Mängel einer zu unbestimmt geregelten oder zu niedrig angesetzten Eingriffsschwelle auszugleichen, da auch die unabhängige Prüfungsinstanz nur sicherstellen kann, dass die geregelten Eingriffsvoraussetzungen eingehalten werden.“; vgl. auch BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 213.

³⁰⁵ Gusy, VerwArch 2015, 437, 450; Gusy, JZ 1998, 167, 172; ähnlich: Waldhoff, Kontrolle, 73, 86, Kutscha, NVwZ 2003, 1296, 1300.

„Wer mangels hinreichender Maßstäbe kein rechtswidriges Verhalten feststellen kann, kann und darf nicht in die Aufgabenerfüllung der Dienste eingreifen. Hier mutiert die angebliche Stärke der offenen Rechtsnormen als Handlungsnormen zu ihrer Schwächung als Kontrollnormen und damit der Kontrollinstanzen. Diese können nicht mehr und nichts anderes an Recht durchsetzen als die maßgeblichen Normen enthalten. Und wenn diese keine hinreichend tauglichen Grenzen ziehen, verwandeln sich die Kontrollverfahren zu bloßer Kontrollkulisse ohne Rechtsschutzgewinn.“³⁰⁶

Eine ausreichend bestimmte gesetzliche Grundlage ist in diesem Verständnis die Basis, auf der Kontrolle aufbaut.³⁰⁷ Zwischen den Verhaltensnormen und der Kontrolle existiert folglich eine Wechselwirkung: Je weiter und unbestimmter die Tatbestandsvoraussetzungen in den Verhaltensnormen ausgestaltet sind, desto oberflächlicher bleibt die Kontrolle. Daraus folgt, dass die Kontrollintensität angehoben werden kann, indem die Befugnisnormen präzisiert werden. Daraus ergibt sich zudem, dass der Gesetzgeber schon zur Ermöglichung der Rechtskontrolle bemüht sein muss, alle Befugnisse der Nachrichtendienste, die in Grundrechte eingreifen, normativ abzubilden und dafür eine gesetzliche Grundlage zu schaffen. Nur wenn es eine (spezifische) gesetzliche Grundlage gibt, kann die Rechtmäßigkeit gehaltvoll kontrolliert werden.

³⁰⁶ Gusy, VerwArch 2015, 437, 450 f. Obwohl viele Nachrichtendienstgesetze nach dem Erscheinen dieses Aufsatzes reformiert wurden und seitdem nähere Angaben zu nachrichtendienstlichen Mitteln enthalten, ist mit den Reformen keine Neustrukturierung der Tatbestände verbunden worden, die dem Aufsatz seine Aktualität nähme.

³⁰⁷ Ähnlich: BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 155: „Das Erfordernis einer an konkrete Umstände anknüpfenden Eingriffsschwelle sichert die Begrenzung von Grundrechtseingriffen, bindet sie an objektivierte Voraussetzungen und ermöglicht eine Kontrolle anhand für sich stehender Kriterien.“; ebenso Kutscha, NVwZ 2003, 1296, 1300: „Grundrechtsschutz durch Verfahren‘ kann nur funktionieren, wenn als Kontrollmaßstab hinreichend bestimmte Regelungen bestehen, anhand derer sich die Zulässigkeit von Eingriffsmaßnahmen der Sicherheitsbehörden beurteilen lässt“; Gusy, JZ 1998, 167, 172; bezogen auf die nur abstrakte Regelung von Observationen Gärditz, EuGRZ 2018, 6, 20.; vgl. auch Sondervotum zu EGMR 25.5.2021 - 58170/13, 62322/14, 24960/15- Big Brother Watch gg. UK, Richter Lemmens, Vehabovic, Bosnjak, Rn. 22: „The crucial point of any prior authorisation is to verify whether the envisaged interference complies with the substantive criteria for such interference. However, if the substantive criteria are vague, overly broad or even non-existent, the requirement of prior authorisation will necessarily fail to provide for sufficiently effective protection against arbitrariness and abuse“.

Fest steht: Eine eigenständig nachrichtendienstliche, detailliertere und stringendere, stärker maßnahmenpezifische³⁰⁸ Befugnisdogmatik ist der zentrale Hebel, um die Rechtskontrolle zu verbessern.³⁰⁹

IV. Intransparenz der Verarbeitung

Dass Betroffene von der heimlichen Maßnahme in Kenntnis gesetzt werden, ist für sie von zentraler Bedeutung, da sie sich nur dann gerichtlich dagegen wehren können. Gem. Art. 19 Abs. 4 GG haben von heimlichen Maßnahmen Betroffene einen Anspruch darauf, nachträglich darüber informiert zu werden. Eine bestimmte Art der Kenntnisgewähr ist nicht vorgeschrieben, sodass grundsätzlich sowohl Auskunftsansprüche als auch Benachrichtigungspflichten denkbar sind. Trotzdem kann eine Pflicht zur Benachrichtigung bestehen, soweit Betroffenen keine Auskunftsansprüche zustehen oder die vorgesehenen Auskunftsansprüche die Betroffenenrechte nicht wahren.³¹⁰

Für eingriffsintensive, heimliche Maßnahmen müssen die nachrichtendienstlichen Fachgesetze grundsätzlich entsprechende Benachrichtigungspflichten enthalten.³¹¹ Allerdings werden die Benachrichtigungspflichten von weitreichenden Ausnahmenvorschriften zum Schutz von Allgemeinwohlinteressen oder Rechtsgüter Dritter flankiert, um im Einzelfall berechnete Geheimschutzinteressen der Nachrichtendienste wahren zu können.³¹² Auch die Auskunft kann aus vergleichbaren Gründen abgelehnt werden.³¹³ Diese Ausnahmen müssen jedoch auf das „erforderliche Maß“ beschränkt

³⁰⁸ Bäcker schlägt eine stärker maßnahmenpezifische Ausgestaltung vor, um hohen Eingriffsintensitäten Rechnung zu tragen, vgl. *Bäcker*, Eingriffstatbestände, 137, 150.

³⁰⁹ So auch Richter am Bundesverfassungsgericht, Andreas Paulus, in der Mündlichen Verhandlung zum Bayerischen Verfassungsschutzgesetz am 14.12.2021, der darauf hinwies, dass eine richterliche Kontrolle Schwellen voraussetzt, da der Richter sonst nicht wissen könne, was er kontrollieren solle.

³¹⁰ *Kornblum*, Rechtsschutz, 234 f. m Verweis auf BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 170; *Wöckel*, Hdb. des Rechts der Nachrichtendienste, 1607, 1623 Rn. 17.

³¹¹ BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 245. Tatsächlich erfüllen nicht alle Gesetze diesen Anspruch, vgl. beispielsweise Bäcker, Verfassungsbeschwerde gegen BayVSG, 1, 51 f.

³¹² BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09, 1 BvR 1140/09 - Rn. 136.

³¹³ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09, 1 BvR 1140/09 - Rn. 137; Bäcker, Verfassungsbeschwerde gegen BayVSG, 1, 54.

sein.³¹⁴ In der Praxis werden die Benachrichtigungen häufig „ausgesetzt“, sodass Betroffene nur ausnahmsweise benachrichtigt werden.³¹⁵ Daher sind die Datenverarbeitungen der Nachrichtendienste trotz der Auskunftsrechte und Benachrichtigungspflichten überwiegend intransparent.³¹⁶ Der „effektiven aufsichtlichen Kontrolle“ komme deshalb „umso größere Bedeutung zu“, betont das Bundesverfassungsgericht.³¹⁷

³¹⁴ BVerfG, Urteil v. 3.3.2004 - 1 BvR 2378/98 - Rn. 292; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 244; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 136; *Bäcker*, Hdb. des Verfassungsrechts, 1715, 1753 Rn. 116.

³¹⁵ *Bantlin*, G 10-Kommission, S. 106, wonach eine Auswertung der Berichte des PKGr ergeben hat, dass die meisten Benachrichtigungen ausgesetzt werden. So auch das Bundesverfassungsgericht in BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 118 und BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 240: „Der Grundsatz der Offenheit der Datenerhebung gilt für sie [die Nachrichtendienste] nicht, und sie sind von Transparenz- und Berichtspflichten gegenüber Betroffenen weithin freigestellt. Entsprechend gering sind die Möglichkeiten individuellen Rechtsschutzes“.

³¹⁶ So u.a. auch *Gusy*, *VerwArch* 2015, 437, 447.

³¹⁷ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 140, vgl. auch BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 273.

Teil 2

Vorgaben für die externe Rechtskontrolle nach höherrangigem Recht

Im folgenden zweiten Teil dieser Untersuchung werden die verfassungs-, völker- und unionsrechtlichen Anforderungen an die Funktionsbestandteile der Rechtskontrolle beschrieben. Die im vorangehenden Kapitel diskutierten Verhaltensnormen können – trotz ihrer Interdependenz mit der Intensität von Kontrolle – in dieser Arbeit nicht weitergehend betrachtet werden.

A. Verfassungsrechtliche Determinanten der externen Rechtskontrolle

„Accountability for power and safeguards against its abuse are not optional extras in the Rechtsstaat, but essential to the legitimacy of the power exercised.“

Iain Cameron, 2020¹

Die Tätigkeit von Sicherheitsbehörden fällt in den Kernbereich staatlicher Souveränität. Aus diesem Grund bietet es sich an, bei der Suche nach Maßstäben für die Nachrichtendienstkontrolle den Blick zuerst auf das deutsche Verfassungsrecht zu richten. Insoweit ist zu klären, wieso die Nachrichtendienste kontrollbedürftig sind (I.) und welche Grundrechte durch ihre Tätigkeit berührt werden (II.). Anschließend werden die Vorgaben des Bundesverfassungsgerichts zur Rechtskontrolle der Nachrichtendienste erläutert (III.) und kritisch diskutiert (IV.).

I. Kontrollbedürfnis

Bevor die verfassungsrechtlichen Determinanten der externen Rechtskontrolle untersucht werden, gilt es eine vorgelagerte Frage verfassungsrechtlich zu beantworten: Die Frage nach dem „Warum“. Weshalb sind die Nachrichtendienste kontrollbedürftig?

¹ Cameron, International Journal of Intelligence and Counterintelligence, 452, 453.

Zunächst lassen sich die Nachrichtendienste unabhängig von ihrem Auftrag abstrakt als ein Teil der Exekutive, das heißt als Verwaltungsbehörden betrachten. Dann stellt sich die Frage, was die staatsrechtliche Begründung dafür ist, dass Verwaltungsbehörden (unabhängig von ihrer konkreten Aufgabe) kontrolliert werden müssen (vgl. 1. und 2.). Blickt man auf die Nachrichtendienste und ihre Tätigkeit, lassen sich aus dem Verfassungsrecht ergänzende Kontrollgründe ableiten (siehe 3.). Die Kontrollbedürftigkeit hat sich in den letzten Jahren noch erhöht (vgl. 4.).

1. Demokratieprinzip

„Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt“, heißt es in Art. 20 Abs. 2 GG. Damit ist das Volk der Träger der Staatsgewalt.² Eine Konsequenz dieses Grundsatzes ist, dass das Volk einzelnen Personen die hoheitliche Gewalt nicht dauerhaft und uneingeschränkt zubilligt, sondern ihnen diese Gewalt lediglich „treuhänderisch“ überträgt.³ Das Volk muss über hinreichend effektive Einflussmöglichkeiten auf staatliches Handeln verfügen, weil diese Einflussmöglichkeiten die staatliche Gewalt erst legitimieren.⁴

Dass dieser Einfluss besteht und staatliche Handlungen inhaltlich an den Volkswillen gebunden sind (sachlich-inhaltliche Legitimation), wird durch periodische Wahlen abgesichert, in denen das Volk die Zusammensetzung des Parlaments bestimmt.⁵ Dieses vom Volk gewählte Parlament kontrolliert die Regierung, die wiederum das Handeln der ihr nachgeordneten Behörden kontrolliert.⁶ In der repräsentativen Demokratie des Grundgesetzes soll diese Kontrolle den Missbrauch der auf Zeit anvertrauten Macht verhindern.⁷ Kontrolle ist somit Ausfluss der sachlich-inhaltlichen demokratischen Legitimation.⁸

² BVerfG, Urteil v. 31.10.1990 - 2 BvF 3/89 - Rn. 48; BVerfG, Beschluss v. 24.5.1995 - 2 BvF 1/92 - Rn. 135.

³ Kempny, Verwaltungskontrolle, S. 1; vgl. auch Scheuner, Verantwortung und Kontrolle, 379, 385.

⁴ BVerfG, Urteil v. 31.10.1990 - 2 BvF 3/89 - Rn. 48; BVerfG, Beschluss v. 24.5.1995 - 2 BvF 1/92 - Rn. 135 f.; Kahl, Kontrolle, 459, 487; Kempny, Verwaltungskontrolle, S. 2: „Verwaltungskontrolle (...) sichert den Einfluss des Volkswillens auf die Ausübung der hoheitlichen Gewalt und trägt damit gleichzeitig zur Legitimation dieser Staatsgewalt bei, die doch, Zwang gegenüber Freien darstellend, nur als Herrschaft des Volkes über sich selbst gerechtfertigt sein kann“ m.w.N.

⁵ Dürig/Herzog/Scholz/Grzeszick, Art. 20 GG Rn. 124 f.; Thomé, Reform der Datenschutzaufsicht, S. 109 ff.; auch Böckenförde, Hdb. des Staatsrechts, § 34 Rn. 19; Scheuner, Verantwortung und Kontrolle, 379, 395, 397.

⁶ Dürig/Herzog/Scholz/Grzeszick, Art. 20 GG Rn. 124 f.; Badura, Legitimation des Verfassungsschutzes, 27, 47.

⁷ Bantlin, G 10-Kommission, S. 86.

⁸ Kahl, Kontrolle, 459, 488 ff. Rn. 65, 68.

2. Rechtsstaatsprinzip

Dass das Verwaltungshandeln kontrolliert werden muss, ergibt sich zudem aus dem Rechtsstaatsprinzip gem. Art. 20 Abs. 3 GG: „Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Recht und Gesetz gebunden.“ Daraus folgt unter anderem das Prinzip der Gesetzmäßigkeit der Verwaltung, also der Vorrang und der Vorbehalt des Gesetzes.⁹ Demnach ist die Exekutive an Gesetze gebunden, hat Parlamentsgesetze vorrangig zu berücksichtigen und darf nur auf Basis einer gesetzlichen Grundlage in Freiheitsrechte eingreifen.¹⁰ Um sicherzustellen, dass diese rechtsstaatlichen Grundsätze eingehalten werden, müssen staatliche Organe kontrolliert werden.¹¹ Folglich ist es der Zweck der Kontrolle, die Gesetzmäßigkeit der Verwaltung durchzusetzen.¹² Kontrolle ist damit selbst ein Gebot des Rechtsstaatsprinzips, denn „rechtsstaatliche Garantien sind im Ernstfall nur so viel Wert wie ihre Kontrolle. Das gilt auch und gerade für die Gesetzmäßigkeit der Verwaltung“.¹³

Eine weitere, für die Herleitung des Kontrollbedürfnisses relevante Garantie des Rechtsstaatsprinzips ist die in Art. 20 Abs. 2 GG verankerte Gewaltenteilung. Die zentrale Vorgabe des Gewaltenteilungsgrundsatzes ist, dass staatliche Gewalt nicht in einer Person oder Institution konzentriert sein darf, sondern auf die Staatsgewalten (Legislative, Exekutive und Judikative) verteilt sein muss.¹⁴ Ein wesentlicher Zweck dieser Aufteilung ist, dass sich die verschiedenen Staatsgewalten gegenseitig in ihrer Gewaltausübung kontrollieren (Gedanke der „checks and balances“).¹⁵ Auf diese Weise soll erstens verhindert werden, dass Macht missbraucht wird.¹⁶ Zweitens soll staatliches Handeln durch die Kontrolle „rationalisiert“ werden, sodass „die inhaltliche Sachrichtigkeit“ der staatlichen Entscheidungen erhöht wird.¹⁷ In diesem Zusammenhang ist eine staatliche Tätigkeit dann „rational“¹⁸, wenn sie den materiellen Vorgaben entspricht, an deren Beachtung die Tätigkeit gebunden ist.¹⁹

⁹ Epping/Hillgruber/Huster/Rux, Art. 20 GG, Rn. 164, 169 f., 172 f.

¹⁰ Dürig/Herzog/Scholz/Grzeszick, Art. 20 GG Rn. 73, 75 f.; Epping/Hillgruber/Huster/Rux, Art. 20 GG Rn. 169 f., 173.

¹¹ Vgl. auch Cameron, International Journal of Intelligence and Counterintelligence 2020, 452, 453.

¹² BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 207: „Sie [die aufsichtliche Kontrolle] dient – neben administrativen Zwecken – der Gewährleistung der Gesetzmäßigkeit der Verwaltung insgesamt (...).“; Schwabenbauer, Heimliche Grundrechtseingriffe, S. 330.

¹³ Sachs, Juridica International 21 (2014), 58, 63; ähnlich Gusy, VerwArch 2015, 437, 439; Nolte, Kontrolle, 11, 17.

¹⁴ Dürig/Herzog/Scholz/Grzeszick, Art. 20 GG Rn. 3091 ff.

¹⁵ Nolte, Kontrolle, 11; Dürig/Herzog/Scholz/Grzeszick, Art. 20 GG Rn. 350 ff.; Hansalek, Parlamentarische Kontrolle, S. 197.

¹⁶ Dürig/Herzog/Scholz/Grzeszick, Art. 20 GG Rn. 35.

¹⁷ Schmidt-Aßmann, Ordnungsidee, S. 212; Krebs, Kontrolle, S. 50; Kabl, Kontrolle, 459, 450.

¹⁸ Zum komplexen Begriff der „Rationalität“, Kempny, Verwaltungskontrolle, S. 30 ff.

¹⁹ Dürig/Herzog/Scholz/Grzeszick, Art. 20 GG Rn. 36.

3. Kompensationsthese

Teilweise wird aus der spezifischen Art ihrer Tätigkeit und bzw. oder den (vergleichsweise) weiten Befugnisnormen hergeleitet, dass die Nachrichtendienste kontrolliert werden müssen. Die Kontrolle diene dazu, die Nachrichtendienste verfassungsrechtlich zu legitimieren.²⁰

a. Kompensation der heimlichen Vorgehensweise

Weil die Nachrichtendienste heimlich arbeiten, sind die Möglichkeiten Betroffener, sich dagegen gerichtlich zur Wehr zu setzen, stark eingeschränkt.²¹ Diese fehlende Rechtsschutzmöglichkeit macht die Ausübung nachrichtendienstlicher Befugnisse besonders kontrollbedürftig²²: „Verfassungsrechtlich hingenommen“ werden könne die Geheimhaltung gegenüber den Betroffenen nach dem Bundesverfassungsgericht „bei der hohen Bedeutung der Grundrechte“ nur, „weil die Kontrolle der Maßnahmen der strategischen Überwachung durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane (Kontrollkommission (...) und Datenschutzbeauftragte) sichergestellt ist“.²³

b. Kompensation gelockerter materieller Bindungen

Darüber hinaus wird teilweise vertreten, die Kontrolle diene der Kompensation unbestimmter Eingriffsermächtigungen^{24, 25}. Anders als die Polizei- und Strafverfolgungsbe-

²⁰ Zum Verfassungsschutz: *Badura*, Legitimation des Verfassungsschutzes, 27, 47; *Hecker*, Hdb. des Rechts der Nachrichtendienste, 222, 229 Rn. 12; *Gusy*, Grundrechte und Verfassungsschutz, S. 11; *Waldhoff*, Kontrolle, 73, 89; *Bantlin*, G 10-Kommission, S. 77, 86 f.

²¹ Vgl. [Teil 1 B. IV.](#)

²² *Gusy*, Grundrechte und Verfassungsschutz, S. 11; *Bantlin*, G 10-Kommission, S. 69-71, 87; *Hecker*, Hdb. des Rechts der Nachrichtendienste, 222, 229 Rn. 12; allgemein bzgl. „heimlicher Ermittlungsmaßnahmen“ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 258; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214; ein Richtervorbehalt könnte dieses „rechtsstaatliche Defizit“ zumindest abmildern, *Bäcker*, Kriminalpräventionsrecht, S. 153; *Alt*, Kompensatorische Kontrolle, S. 3.

²³ BVerfG, Beschluss vom 20.6.1984 - 1 BvR 1494/78 - Rn. 75; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 273.

²⁴ Vgl. [Teil 1 B. III. 3.](#)

²⁵ *Bantlin*, G 10-Kommission, S. 73, 87; *Hecker*, Hdb. des Rechts der Nachrichtendienste, 222, 229 Rn. 12; bezüglich der parlamentarischen Kontrolle wurde dies schon früh vertreten: „Die mehrfach berührte Unbestimmtheit des Maßstabs einer Kontrolle der Dienste mangels Präzisierung der Eingriffsbefugnisse könnte in etwa durch eine solche ‚parlamentarische Kontrolle‘ kompensiert werden, indem in einer solchen Kooperation der Regierung mit einem vom Parlament bestellten Gremium versucht werden

hörden verfügten die Nachrichtendienste über „beträchtliche Entscheidungsfreiräume“. ²⁶ Dieses hohe Maß an Unbestimmtheit verringere die „Legitimationswirkung“ des Gesetzes für die Handlungen der Exekutive. ²⁷ Während das Bundesverfassungsgericht dies früher kritisch sah ²⁸, hat es sich dieser Auffassung mittlerweile angeschlossen: wegen „tatbestandlich weniger scharf konturierter Eingriffsschwellen“ im Nachrichtendienstrecht entstehe ein „besonderer Bedarf nach einer unabhängigen Vorabkontrolle“. ²⁹ Dieses Kompensationsbedürfnis bestehe insbesondere bei strategischen Überwachungen, da diese gesetzlich „im Wesentlichen nur final“ angeleitet würden, Sorge die Kontrolle für die „gebotene verfahrensmäßige Strukturierung der Handhabung“ bei der praktischen Umsetzung. ³⁰

Dagegen spricht, dass die Rechtskontrolle selbst maßgeblich von der Ausgestaltung der Verhaltensnormen abhängig ist. ³¹ Die Kontrolle kann nicht losgelöst von den Befugnisnormen (auch) als Komponente für deren Rechtfertigung dienen, wenn die Wirksamkeit der Kontrolle ihrerseits maßgeblich von den Befugnisnormen abhängig ist. Die Kontrolle ist „nicht geeignet, die Mängel einer zu unbestimmt geregelten oder zu niedrig angesetzten Eingriffsschwelle auszugleichen, da auch die unabhängige Prüfungsinstanz nur sicherstellen kann, dass die geregelten Eingriffsvoraussetzungen eingehalten werden.“ ³²

Unabhängige Rechtskontrollen können die weiten Befugnisnormen somit richtigerweise nicht kompensieren. ³³

4. Steigerung der Kontrollbedürftigkeit

In den letzten Jahrzehnten ist die Verfügbarkeit personenbezogener Daten exorbitant gestiegen: nahezu jede menschliche Bewegung oder soziale Interaktion wird heutzutage auch digital erfasst. Damit stehen den Nachrichtendiensten deutlich mehr Daten zur

könnte, die Voraussetzungen für den Einsatz bestimmter nachrichtendienstlicher Mittel näher zu bestimmen (...)“, *Friesenbahn*, Kontrolle, 87, 99 m. Verweis auf *Borgs-Maciejewski*, Unzulängliche Kontrolle 1977.

²⁶ Hecker, Hdb. des Rechts der Nachrichtendienste, 222, 229 Rn. 12.

²⁷ Gusy, Grundrechte und Verfassungsschutz, S. 130; vgl. auch *Kabl*, Kontrolle, 459, 488 Rn. 66.

²⁸ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 258.

²⁹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 213, 219.

³⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 273.

³¹ Vgl. [Teil 1 B. III. 4.](#)

³² BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 258; bezogen auf die Rechtskontrolle auch *Gusy*, Grundrechte und Verfassungsschutz, S.11; *Bäcker*, K&R 2014, 556; bezüglich des Richtervorbehalts, *Bäcker*, Kriminalpräventionsrecht, S. 156.

³³ Gusy wirft die Frage auf, ob Kontrollen durch das Parlament insoweit legitimationskompensierend wirken können, *Gusy*, Grundrechte und Verfassungsschutz, S. 130. Er begründet diese Überlegung allerdings nicht näher. Nichtsdestotrotz wird dem Vorabkontrolleur diese Aufgabe übertragen, vgl. [Teil 2 A. IV. 2. c.](#)

Verfügung als früher, ihr Potenzial „hat nur noch wenig zu tun mit dem vor 60 Jahren“. Heute wäre – anders als früher – eine verfassungsrechtlich nicht mehr rechtfertigbare Totalüberwachung jedenfalls theoretisch möglich. Diese „gesteigerte Reichweite“ nachrichtendienstlicher Tätigkeit erhöht auch ihren Kontrollbedarf.³⁴

5. Fazit

Im Ergebnis ist die Kontrollbedürftigkeit nachrichtendienstlicher Tätigkeit zunächst eine Konsequenz der heimlichen Vorgehensweise: Die Kontrolle kompensiert den besonders grundrechtsgefährdenden, weil geheimen, Modus Operandi. Darüber hinaus folgt die Notwendigkeit, das Verwaltungshandeln auf seine Rechtmäßigkeit hin zu kontrollieren, vor allem aus dem Rechtsstaatsprinzip. Mit der gestiegenen Reichweite von nachrichtendienstlichen Befugnissen hat sich zudem auch ihre Kontrollbedürftigkeit erhöht.

II. Einschlägige Grundrechte

Das Grundgesetz beinhaltet keine speziellen staatsorganisatorischen Vorgaben dazu, wie die externe Rechtskontrolle über die Nachrichtendienste ausgestaltet sein sollte. Hierin liegt ein wesentlicher Unterschied zur parlamentarischen Kontrolle, für die in Art. 45 d GG bestimmte Mindestvoraussetzungen normiert sind.³⁵ Die verfassungsrechtlichen Anforderungen an die Rechtskontrolle der Nachrichtendienste werden deshalb ausschließlich aus den durch die nachrichtendienstliche Tätigkeit betroffenen Grundrechten abgeleitet.

Das setzt voraus, dass die Nachrichtendienste an die Grundrechte gebunden sind. Weil die Nachrichtendienste Verwaltungsbehörden sind, sind sie gem. Art. 1 Abs. 3 GG an Grundrechte gebunden. Allerdings war lange Zeit umstritten, inwieweit dies gilt, wenn die Nachrichtendienste im Ausland gegenüber Ausländern handeln.³⁶ Art. 1 Abs. 3 GG trifft keine ausdrückliche Aussage zur territorialen Reichweite. Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Auslands-Fernmeldeaufklärung im Jahr 2020 entschieden, dass Art. 1 Abs. 3 GG territorial nicht begrenzt ist und dass die deutsche Staatsgewalt damit stets „umfassend“ an Grundrechte gebunden ist. Dies gelte „jedenfalls für die Grundrechte als Abwehrrechte gegenüber Überwachungsmaßnahmen“. Die Schutzwirkung könne im Ausland jedoch geringer sein.³⁷

³⁴ Masing, Nachrichtendienste, 3, 4, 6, 12.

³⁵ Grundgesetzänderung von 2009, Singer, Art. 45 d GG, Rn. 55, 57.

³⁶ Deutsche Personen sind auch im Ausland geschützt, Schneider, Fernmeldegeheimnis, S. 239.

³⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 88 ff., 104; a. A. früher im Schrifttum beispielsweise Gärditz, Die Verwaltung 2015, 463, 474 f.

Da die nachrichtendienstlichen Befugnisse³⁸ eine große Bandbreite entfalten, können sie potenziell eine Vielzahl von Grundrechten beeinträchtigen.

Die gesetzlichen Ermächtigungen erlauben den Nachrichtendiensten zunächst Eingriffe in Art. 10 GG, der das Brief-, Post- und Fernmeldegeheimnis schützt. Betroffen sind alle drei dieser von Art. 10 garantierten Grundrechte, wobei das Fernmeldegeheimnis in der digitalisierten Welt eine herausragende Bedeutung erlangt hat³⁹. Der sachliche Schutzbereich des Fernmeldegeheimnisses beinhaltet die Vertraulichkeit von Inhalten und Umständen der unkörperlichen Kommunikation an individuelle Empfänger über den Telekommunikationsverkehr.⁴⁰ Der Gewährleistungsbereich ist technologieneutral und entwicklungsoffen.⁴¹ Aus Art. 10 GG ist der Anspruch eines Betroffenen ableitbar, grundsätzlich Kenntnis von einer Datenverarbeitung durch staatliche Stellen zu erlangen.⁴²

Zudem verarbeiten alle Nachrichtendienste personenbezogene Daten, weshalb der Schutzbereich des Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (im Folgenden: RaiS) eröffnet ist. Soweit der Anwendungsbereich des Fernmeldegeheimnisses eröffnet ist, wirkt Art. 10 GG als spezielle Ausprägung des RaiS, die vorrangig anzuwenden ist und das RaiS verdrängt.⁴³

Darüber hinaus ist das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme relevant, das ebenfalls aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG hergeleitet wird. Während Art. 10 Abs. 1 GG als *lex specialis* den laufenden Kommunikationsvorgang schützt, erfasst das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme Eingriffe in komplexe Systeme als solche unabhängig und außerhalb von konkreter Individualkommunikation. Wenn personenbezogene Daten in einem informationstechnischen System betroffen sind, ist das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme vorrangig vor dem einzelne Datenerhebungen schützenden RaiS zu prüfen. Der Schutzbereich beinhaltet sowohl die Vertraulichkeit, also den Schutz vor Kenntnisaufnahme der gespeicherten Informationen durch unberechtigte Dritte, als auch die Integrität, das heißt den Schutz vor Systemveränderung durch unberechtigte Dritte.⁴⁴

³⁸ Vgl. [Teil 1 B. III.](#)

³⁹ Tanneberger, Sicherheitsverfassung, S. 188; Dürig/Herzog/Scholz/Durner, Art. 10 GG Rn. 109.

⁴⁰ BVerfG, Beschluss v. 20.6.1984 - 1 BvR 1494/78 - Rn. 46, 75; BVerfG, Beschluss v. 9.10.2002 - 1 BvR 1611/96 - Rn. 23; BVerfG, Urteil v. 2.3.2010, 1 BvR 256/08 - Rn. 189; Dürig/Herzog/Scholz/Durner, Art. 10 GG Rn. 106.

⁴¹ Dürig/Herzog/Scholz/Durner, Art. 10 GG Rn. 108.

⁴² BVerfG, Beschluss v. 20.9.2016 - 2 BvE 5/15 - Rn. 36, entsprechendes gilt im Anwendungsbereich des RaiS.

⁴³ BVerfG, Beschluss v. 20.6.1984 - 1 BvR 1494/78; BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 Rn. 158; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 Rn. 191.

⁴⁴ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 167 ff., 182 ff., 200 ff.; Bantlin, JuS 2019, 669, 670.

Art. 19 Abs. 4 GG garantiert dem Einzelnen, staatliche Eingriffe vor Gericht auf ihre Rechtmäßigkeit überprüfen lassen zu können. Art. 10 Abs. 2 S. 2 GG modifiziert Art. 19 Abs. 4 GG für bestimmte Aufgaben der Nachrichtendienste.⁴⁵ Demnach kann gesetzlich bestimmt werden, dass Eingriffe Betroffenen nicht mitgeteilt werden und an die Stelle des Rechtsweges die „Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt“. Darüber hinaus stellt Art. 19 Abs. 4 GG i. V. m. dem jeweils einschlägigen Grundrecht bestimmte Anforderungen an den individuellen Rechtsschutz und die Kontrolle.⁴⁶

Art. 13 GG schützt den räumlichen Bereich, in dem das Privatleben stattfindet.⁴⁷ Beim Einsatz nachrichtendienstlicher Mittel in Wohnungen oder Geschäftsräumen ist mithin Art. 13 GG anwendbar. Mit einer Verfassungsänderung im Jahr 1998 wurde Art. 13 GG um weitere Absätze ergänzt.⁴⁸ Seitdem dürfen unter anderem gem. Art. 13 Abs. 4 GG zwar technische Mittel zur Wohnungsüberwachung zwecks Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, eingesetzt werden, sie müssen jedoch vorab gerichtlich genehmigt worden sein.

Außerdem können sowohl die Garantien aus Art. 5 Abs. 1 S. 2 GG als auch aus Art. 12 Abs. 1 GG betroffen sein. Denkbar sind zudem Eingriffe in die Parteienfreiheit (Art. 21 GG), den Schutz der Familie (Art. 6 GG) oder die Selbstbelastungsfreiheit als Teil des Rechts auf ein faires Verfahren (Art. 2 Abs. 1 GG i. V. m. Art. 20 Abs. 3 GG).⁴⁹

Zudem können nachrichtendienstliche Befugnisse die Menschenwürde gem. Art. 1 Abs. 1 GG berühren. Ein Eingriff in die Menschenwürde ist vor allem in dessen Ausprägung als Schutz des Kernbereichs privater Lebensgestaltung denkbar. Dieser soll dem einzelnen Bürger einen „Bereich höchstpersönlicher Privatheit gegenüber Überwachung“ garantieren.⁵⁰ Davon umfasst ist die Möglichkeit, im privaten Bereich innere Vorgänge, wie beispielsweise Gefühle und Gedanken höchstpersönlicher Art mit Ehepartnern, engen Freunden oder vergleichbaren Vertrauenspersonen auszutauschen, wenn man berechtigterweise darauf vertrauen durfte, in diesem Moment nicht überwacht zu sein. Der Kernbereich privater Lebensgestaltung ist jedoch kein separates Grundrecht, sondern wird in Verbindung mit den durch die jeweilige Überwachungsbefugnis betroffenen Grundrechten relevant.⁵¹

⁴⁵ Vgl. [Teil 2 A. III. 3. a.](#)

⁴⁶ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 134.

⁴⁷ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 192.

⁴⁸ BT-Drs. 13/8650, Entwurf eines Gesetzes zur Änderung des Grundgesetzes (Artikel 13 GG) v. 1.10.1997; Epping/Hillgruber/*Kluckert*, Art. 13 GG Rn. 15.

⁴⁹ *Hong*, Einsatz von V-Leuten und verdeckten Mitarbeitern, 45, 48.

⁵⁰ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09, 1 BvR 1140/09 - Rn. 120.

⁵¹ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09, 1 BvR 1140/09 - Rn. 121 m. Verweis auf st. Rspr.

Bei der Wohnraumüberwachung ist der Kernbereich demnach im Rahmen von Art. 13 GG zu prüfen, bei Telekommunikationsüberwachungen in Kombination mit Art. 10 GG.⁵²

III. Vorgaben des Bundesverfassungsgerichts

1. Duales Kontrollkonzept des BVerfG: Richterliche bzw. richterähnliche Vorabkontrolle und nachträgliche Datenschutzkontrolle

Rekapituliert man die Judikate des Bundesverfassungsgerichts, zeigt sich ein roter Faden von Mindestvoraussetzungen, die eine verfassungsgemäße Kontrolle nachrichtendienstlicher Maßnahmen zu erfüllen hat. Obgleich die angegriffenen Fachgesetze und Normen sich unterscheiden, greift das Gericht wiederholt auf zwei Arten von Kontrollen zurück: Die richterliche oder richterähnliche unabhängige Vorabkontrolle⁵³ und die Datenschutzkontrolle (bzw. „administrative Kontrolle“ oder „aufsichtliche Kontrolle“⁵⁴). In der neueren Rechtsprechung werden beide Kontrollarten gemeinsam gedacht und einander ergänzend eingesetzt.⁵⁵

⁵² *Schneider*, JuS 2021, 29.

⁵³ Zu den Vorteilen einer unabhängigen richterähnlichen Vorabkontrolle *Venedig-Kommission*, Report 2015, S. 46 f. Rn. 214: „Nonetheless, there is an obvious advantage of requiring prior judicial authorization for special investigative techniques, namely that the security agency has to go “outside of itself” and convince an independent person of the need for a particular measure. It subordinates security concerns to the law, and as such it serves to institutionalize respect for the law. If it works properly, judicial authorization will have a preventive effect.“ In den folgenden Rn. ergänzt die Venedig-Kommission einschränkend, dass die Effektivität von der Unabhängigkeit und Expertise der Mitglieder abhängig ist.

⁵⁴ Das BVerfG variiert die Begrifflichkeiten, bezeichnet damit aber immer die nachträgliche Rechtmäßigkeitskontrolle von Datenverarbeitungen (zur „administrativen Kontrolle“ in BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276, zur „aufsichtlichen Kontrolle“ u.a. in BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 214 ff., BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290). Im Folgenden wird zur Vereinfachung der Begriff „Datenschutzkontrolle“ verwendet.

⁵⁵ Beide gemeinsam thematisiert z.B. in BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 279: „Im Zusammenwirken der Kontrollinstanzen muss gewährleistet sein, dass der gesamte Prozess der strategischen Überwachung (...) potenziell umfassend der Kontrolle unterliegt. Soweit keine gerichtssähnliche Kontrolle vorgesehen ist, muss die Möglichkeit der administrativen Kontrolle eröffnet sein.“ Der Verfahrensgegenstand von BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - zählt zwar zum Polizeirecht, die Entscheidung kann dennoch im Folgenden zitiert werden, weil die Senatsmehrheit die Anforderungen an eine verhältnismäßige Befugnisgestaltung heimlicher Maßnahmen nicht nur für das Polizeirecht, sondern rechtsgebietsübergreifend für das gesamte Sicherheitsrecht etabliert. Dies verdeutlicht unter anderem der Wortlaut, wonach der Senat „übergreifende Anforderungen“ für heimliche, tief in die Privatsphäre eingreifende Befugnisse formuliert. Innerhalb der abstrakt zu den Standards formulierten Ausführungen bezieht das Gericht sich nicht auf das Polizeirecht. Bezugspunkt sind allein die heimlichen Befugnisse. In seinem Urteil zur strategischen Ausland-Fernmeldeüberwachung hat das Bundesverfassungsgericht diese Interpretation erstmals bestätigt, sodass an der Übertragbarkeit keine Zweifel bestehen (BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 141).

Deren Gemeinsamkeiten und Unterschiede mit Hilfe des verwaltungswissenschaftlichen Instrumentariums zur Analyse von Kontrollstrukturen⁵⁶ herauszuarbeiten, ist das Ziel dieses Abschnitts.

a. Grundsatz

Das Bundesverfassungsgericht formuliert grundsätzliche Vorgaben des dualen Kontrollkonzepts (a.), die es für die strategische Ausland-Fernmeldeüberwachung detailliert (b.).

aa) Kontrollmaßstab

Die richterliche oder richterähnliche unabhängige Vorabkontrolle und die Datenschutzkontrolle verbindet, dass es sich bei ihnen um „Rechtskontrolle“ handelt.⁵⁷

bb) Zeitpunkt

Die Kontrollmodi unterscheiden sich jedoch durch den *Zeitpunkt* der Kontrolle. Die unabhängige bzw. richterliche Kontrolle soll *ex ante* über die Zulässigkeit einer Maßnahme entscheiden.⁵⁸ In Eilfällen kann auf die *ex ante*-Kontrolle verzichtet werden, dann muss jedoch eine nachträgliche Kontrolle durch eine unabhängige Stelle erfolgen.⁵⁹

Die Datenschutzkontrolle erfolgt später als die Vorabkontrolle, sie ist während der Datenverarbeitung bis nach ihrem Abschluss möglich.⁶⁰

⁵⁶ Vgl. [Teil 1 A. III.](#)

⁵⁷ Das BVerfG stellt wiederholt explizit auf diesen Begriff ab, vgl. BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 77; BVerfG, Beschluss v. 20. September 2016 - 2 BvE 5/15 - 1 Rn. 38; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 76; in BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 171 heißt es über den Prüfungsumfang der Kontrollen im Anwendungsbereich von Art. 10: „Kontrollbedürftig ist sowohl die Rechtmäßigkeit der Eingriffe als auch die Einhaltung der gesetzlichen Vorkehrungen zum Schutz des Fernmeldegeheimnisses“.

⁵⁸ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 77; BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 257, 259; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 248; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 117 f.; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 275; BVerfG, Urteil v. 26.4.2022, 1 BvR 1619/17 Rn. 214; BVerfG, Beschluss v. 10.11.2020 - 1 BvR 3214/15 - Rn. 135.

⁵⁹ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 261; der Gesetzgeber habe den Raum, für „Ausnahmefälle bei Gefahr im Verzug“ „besondere Regelungen“ zu treffen, BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 361.

⁶⁰ Kontrolle der „Anwendung“ in BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 184; Protokollierung der Erhebung setzt voraus, dass sie noch erfolgt bzw. schon erfolgt ist in BVerfG, Urteil v. 20.4.2016

cc) Kontrolleur

Welche konkrete Institution der Gesetzgeber als *Kontrolleur* einsetzt, liegt weitgehend im Regelungsspielraum des Gesetzgebers.

Bei der Vorabkontrolle legt das Bundesverfassungsgericht sich auf eine gerichtliche oder richterähnliche Kontrollinstitution fest.⁶¹ Da es in fast⁶² allen Urteilen eine „richterähnliche“ Alternative zur gerichtlichen Kontrolle als verfassungsrechtlich zulässig erachtet, kommt dem Gesetzgeber insoweit auch bei der Vorabkontrolle ein Regelungsspielraum zu.⁶³ Davon ausgenommen ist der Anwendungsbereich von Art. 13 GG, in dem wegen dessen Abs. 3 - 4 nur ein Richtervorbehalt verfassungsgemäß ist.

Soweit bei der Datenschutzkontrolle die Datenschutzbeauftragten als konkrete Kontrollinstitutionen erwähnt werden, werden diese lediglich als Beispiel für eine verfassungskonforme Ausgestaltungsmöglichkeit der Datenschutzaufsicht angeführt.⁶⁴

- 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 141, 266; ebenfalls kein Zeitpunkt definiert in BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276, BVerfG, Urteil v. 26.4.2022 - 1619/17 - Rn. 290.

⁶¹ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 - Rn. 77; BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259 f.; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 248; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 117 f.; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 Rn. 275; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 Rn. 214, 224.

⁶² Diese Möglichkeit wurde in BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 nicht explizit erwähnt. Dagegen, dass von der Alternative einer vergleichbar neutralen, richterähnlichen Vorabkontrolle abgewichen werden sollte, spricht, dass das Gericht die Kontrolle gem. Art. 10 Abs. 2 S. 2 GG ausdrücklich anspricht. Aufgrund dieser speziellen Normierung im Anwendungsbereich von Art. 10 GG ist es nicht notwendig, auf andere Optionen hinzuweisen. Jedenfalls kommt das Gericht in späteren Urteilen auf die alternative Vorabkontrolle durch eine unabhängige Stelle zurück, was belegt, dass eine Rechtsprechungsänderung nicht intendiert war.

⁶³ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 Rn. 171: „Wie die Kontrolle auszugestalten ist, schreibt die Verfassung jedoch nicht vor. Dem Gesetzgeber steht es frei, die ihm geeignet erscheinende Form zu wählen, wenn sie nur hinreichend wirksam ist.“; BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 260; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 117 f.; BVerfG, Beschluss v. 20.9.2016 - 2 BvE 5/15 - Rn. 403; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214, 224. In BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 271 schreibt das Gericht, Art. 10 Abs. 2 S. 2 GG enthalte „keine detaillierte Organisationsanleitung“, die Besetzung müsse lediglich unter Beachtung der verschiedenen im Parlament vertretenen Fraktionen bestimmt werden, es sei nicht zwingend, dass Bundestagsabgeordnete darunter vertreten seien, vielmehr könne das Kontrollorgan innerhalb oder außerhalb des Parlaments und sogar organisatorisch als Organ der Exekutive ausgestaltet werden.

⁶⁴ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 215; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 141; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276, 282; *Siems*, NWVbl 2018, 1, 6; *Schenke/Graulich/Ruthig/Siems*, § 26a BVerfSchG Rn. 6, anders im nicht auf die Nachrichtendienstbezogenen Volkszählungsurteil, BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83 - Rn. 155, in dem das Gericht explizit von der Beteiligung „unabhängiger Datenschutzbeauftragter“ spricht. In der Literatur überwiegt diesbezüglich die Auffassung, dass das BVerfG den Datenschutzbeauftragten nur beispielhaft benannt habe und die institutionelle Ausgestaltung der Datenschutzkontrolle im Regelungsspielraum des Gesetzgebers verbleiben sollte, *Dürig/Herzog/Scholz/Di Fabio*, Art. 2 GG Rn. 184.

dd) Distanz

Das Bundesverfassungsgericht hebt hervor, dass die Vorabkontrolleure (weisungsfrei und) unabhängig sein sollen⁶⁵ und äußert sich somit zur notwendigen *Distanz*. Die Kontrolleure sollen insbesondere vor Weisungen der Exekutive geschützt werden und nur dem Gesetz unterworfen sein.⁶⁶ Die Kontrolle durch ein Gericht oder eine richterähnliche Institution ordnet das Bundesverfassungsgericht als die die Unabhängigkeit bestmöglich wahrende Kontrolloption ein⁶⁷; deshalb solle die *ex ante-Kontrolle* richterlich bzw. richterähnlich konzipiert sein.

Die Datenschutzkontrolle solle ebenfalls „unabhängig“ sein.⁶⁸

ee) Modalitäten

Betrachtet man die *Modalitäten* der Kontrolle, zeigen sich Unterschiede. Die Vorabkontroll-Institution hat in jedem Einzelfall und dauerhaft über die Zulässigkeit einer Maßnahme zu entscheiden.⁶⁹

Die Genehmigung durch einen unabhängigen Vorabkontrolleur muss nur bei eingriffsintensiven Maßnahmen erteilt werden.⁷⁰ Weniger eingriffsintensive Maßnahmen, die ursprünglich keiner Genehmigung bedurften, können nachträglich genehmigungspflichtig werden: Soweit die Maßnahme lange andauere, könne die Eingriffsintensität so weit ansteigen, dass die unabhängige Genehmigung zu einem späteren Zeitpunkt nachgeholt werden muss.⁷¹ Das bedeutet, dass die Eingriffsintensität solcher Maßnahmen laufend evaluiert werden muss.

⁶⁵ Zur Vorabkontrolle: u.a. in BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 - Rn. 77 (hier heißt zusätzlich, das Organ könne „innerhalb oder außerhalb des Parlaments“ gebildet werden), BVerfG, Beschluss vom 20.6.1984 - 1 BvR 1494/78 - Rn. 75; BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 171; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 117; Gusy, Grundrechte und Verfassungsschutz 2011, S. 34.

⁶⁶ Auf Grundlage dieser Rechtsprechung (vgl. vorige Fn.) Gusy, Grundrechte und Verfassungsschutz, S. 35 f., wonach nicht nur Weisungen im Einzelfall, sondern auch Verwaltungsvorschriften davon erfasst sind.

⁶⁷ Explizit so formuliert in BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259, 260, „gleiche Gewähr für ihre Unabhängigkeit und Neutralität (...) wie ein Richter“.

⁶⁸ BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83 - Rn. 155; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 281.

⁶⁹ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 - Rn. 77, „laufend“; ergibt sich daraus, dass das Gericht auf die einzelne Maßnahme abstellt, für die eine Vorabkontrolle erforderlich ist und diese demnach auf alle Maßnahmen bezieht, u.a. in BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 217; BVerfG, Beschluss v. 20.9.2016 - 2 BvF 5/15 - Rn. 38.

⁷⁰ Vgl. [Teil 2 A. III. 3. d. cc](#).

⁷¹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 220.

Darüber hinaus müssten länger andauernde Eingriffe, die vorab unabhängig kontrolliert worden seien, entweder befristet oder nochmals kontrolliert werden. Die Kontrolle, die „eine vorausschauende Beurteilung der Effektivität“ einer Maßnahme beinhalten müsse, könne „im Hinblick auf den einschneidenden Eingriff einerseits und die hochrangigen Rechtsgüter andererseits hinreichend verantwortungsvoll nur für einen überschaubaren Zeitraum vorgenommen werden.“⁷²

Die Datenschutzkontrolle hingegen erfolgt stichprobenartig. Das Bundesverfassungsgericht fordert ein „regelmäßiges“ Intervall von maximal zwei Jahren zwischen den Stichprobenkontrollen.⁷³

ff) Initiative

Wer *initiativberechtigt* ist, beschreibt das Bundesverfassungsgericht weniger eindeutig. Die Antwort auf diese Frage lässt sich jedoch teilweise aus der Rechtsprechung ableiten. Wenn die Vorabkontrollinstanz über die Zulässigkeit der jeweiligen Maßnahmen entscheiden soll, muss sie von der Behörde zunächst vorab über die geplante Maßnahme in Kenntnis gesetzt werden. Denn es ist die Nachrichtendienstbehörde, die über den Einsatz bestimmter Befugnisse Beschluss fasst und dazu jeweils die Genehmigung der Kontrollinstanz einholen muss. Bei der Vorabkontrolle geht die Kontrollinitiative somit von den Nachrichtendiensten aus.

Die Datenschutzkontrolle, schreibt der Senat in der Entscheidung zur strategischen Ausland-Fernmeldeaufklärung vom 19. Mai 2020, solle von der administrativen Kontrollinstanz „eigeninitiativ“ durchgeführt werden.⁷⁴ In anderen Urteilen äußert sich das Gericht dazu nicht. Möglicherweise wollte das Bundesverfassungsgericht eine Initiativberechtigung der Datenschutzaufsicht außerhalb der strategischen Ausland-Fernmeldeaufklärung nicht konstituieren. Dafür spricht, dass das Gericht die strategische Überwachung insgesamt detaillierter reguliert, sich die Vorgabe der „eigeninitiativen“ Kontrolle insoweit nahtlos in die Argumentation einfügt und dies die Position des Kontrolleurs stärkt, was bei den anderen Befugnissen möglicherweise nicht intendiert war.

Demgegenüber spricht für eine generelle Initiativberechtigung des Datenschutzkontrolleurs, dass die Initiative für eine unabhängige „Stichprobenkontrolle“ vom Kontrolleur ausgehen sollte, um ihren Zweck zu realisieren. Der Sinn, den das Gericht der Datenschutzkontrolle zuschreibt, besteht unter anderem darin, den Ausfall von subjektiven Rechtsschutzmöglichkeiten zu kompensieren, was die Wirksamkeit des Kontrollmechanismus voraussetzt. Würde stattdessen der Kontrollierte über den Zeitpunkt und

⁷² BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 220.

⁷³ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 217; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 141.

⁷⁴ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276.

den Gegenstand der Stichprobenkontrolle entscheiden, wären die Kontrollen unwirksam, weil er den *Ist-Zustand* noch zu seinem Vorteil anpassen könnte. Letztlich muss unter dem Gesichtspunkt der Wirksamkeit daher der Datenschutzkontrolleur initiativberechtigt sein.

gg) Kontrollmittel zur Informationsgewinnung

Die Anforderungen an die *Informationsgewinnung* der Kontrollinstitutionen beschreibt das Bundesverfassungsgericht bei beiden Kontrollmodi ähnlich: Zunächst sollen die nachrichtendienstlichen Entscheidungen substantiiert begründet und dabei alle „beurteilungsrelevanten Aspekte“⁷⁵ offengelegt sowie die Datenverarbeitungen zu Kontrollzwecken umfassend protokolliert werden.⁷⁶ Die Protokollierungspflicht zu Kontrollzwecken ergibt nur dann Sinn, wenn der Kontrolleur ein Auskunfts- und Einsichtsrecht hat und so Kenntnis von den Protokollen erlangen kann. Ob die Entscheidungsgrundlagen dokumentiert werden müssen, ist von der Eingriffsintensität abhängig, so müssen die rechtlichen und tatsächlichen Grundlagen bei einer geringen Eingriffsintensität nicht festgehalten werden.⁷⁷

Der Vorabkontrolleur solle über den Sachstand umfassend informiert werden, der Antrag der kontrollierenden Behörde müsse substantiiert begründet und vor allem begrenzt sein.⁷⁸

⁷⁵ Zur richterähnlichen Kontrolle, BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 215.

⁷⁶ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 280 (hier bezogen auf Datenübermittlungen); BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 184, 215, die für die Anwendung der Antiterrordatei im Einzelfall maßgeblichen Kriterien müssten abstrakt-generell festgelegt, dokumentiert und gegenüber den Kontrolleuren offengelegt werden. Dieses Vorgehen sichere „ein hinreichendes Kontrollniveau“ und ersetze „insbesondere die Datenschutzbeauftragten in die Lage, zu kontrollieren, ob die (...) Anwendung der Vorschriften durch die Exekutive rationalen Kriterien folgt und durch Sinn und Zweck des Gesetzes geleitet ist“; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 118, 141, 266, insbesondere dürften die Protokolle von Löschungen so lange nicht vernichtet werden, dass sie innerhalb der Frist der turnusmäßigen Kontrolle bei typisierender Betrachtung durch die Datenschutzbeauftragten und einer möglichen Benachrichtigung des Betroffenen noch vorlägen.

⁷⁷ BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 248 ff. Bedeutend ist dies nur für die Datenschutzkontrolle, da bei geringer Eingriffsintensität keine Vorabkontrolle vorgeschrieben ist. Dass insoweit nach der Eingriffsintensität unterschieden wird, ist nicht überzeugend: Da das Bundesverfassungsgericht bei jeder Datenverarbeitung Kontrollen verlangt, müssen diese über eine behördliche Dokumentation ermöglicht werden.

⁷⁸ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 117 f.; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 215.

Den Datenschutzkontrolleuren müssten die Daten in „praktikabel auswertbarer Weise“ zur Verfügung gestellt werden und die Protokolle müssten so gestaltet sein, dass sie einem Datenverarbeitungsvorgang zuordenbar sind.⁷⁹

Die Datenschutzkontrolleure seien zudem mit wirksamen Befugnissen auszustatten.⁸⁰ Was unter „wirksamen Befugnissen“ zu verstehen ist, konkretisiert das Bundesverfassungsgericht nicht. Dies festzulegen, bleibt dem Gesetzgeber überlassen. Dennoch stellt sich die Frage, ob damit ein Mindestbestand an Befugnissen impliziert ist. Einen konkreten Mindestbestand an Befugnissen hat das Bundesverfassungsgericht nicht definiert, feststeht aber, dass der Datenschutzkontrolleur mit Befugnissen – das Gericht verwendet hier den Plural – auszustatten ist. Dem Kontrolleur keine Befugnisse einzuräumen, wäre damit verfassungswidrig. „Wirksam“ bedeutet, „eine beabsichtigte Wirkung erzielend“ oder „mit Erfolg wirkend“.⁸¹ Die dem Datenschutzkontrolleur verliehenen Befugnisse müssen deshalb so ausgestaltet sein, dass der beabsichtigte Erfolg tatsächlich eintritt.

Aus der Protokollierungspflicht zu Kontrollzwecken folgt, dass mindestens Auskunfts- und Einsichtsrechte vorzusehen sind. Diese Auskunfts- und Einsichtsrechte müssen so ausgestaltet sein, dass der Kontrolleur die Daten tatsächlich einsehen und dieses Recht in Zweifelsfällen auch durchsetzen kann. Nur dann sind sie „wirksam“.

hh) Kontrollergesultfolge

Ein wesentlicher Unterschied zwischen den beiden Kontrollmodi besteht bei den jeweils möglichen *Kontrollergesultfolge*. Die richterliche bzw. richterähnliche Vorabkontrolle ist nach der Rechtsprechung des Bundesverfassungsgerichts mit einem abschließenden Entscheidungsrecht auszustatten, das heißt, wenn und soweit sie eine Maßnahme genehmigt, kann diese erfolgen; lehnt sie die Genehmigung ab, muss der Nachrichtendienst von der Maßnahme absehen.⁸²

⁷⁹ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 214 f; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 Rn. 141; Zugang zu „entscheidungserheblichen“ Unterlagen in BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 77.

⁸⁰ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 215; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 Rn. 141, 266, identischen Formulierungen in beiden: „Die Gewährleistung einer wirksamen Aufsicht setzt zunächst sowohl auf Bundes- wie auf Landesebene mit wirksamen Befugnissen ausgestattete Aufsichtsinstanzen – wie nach geltendem Recht die Datenschutzbeauftragten – voraus.“; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

⁸¹ <https://www.duden.de/rechtschreibung/wirksam> (abgerufen am 31.8.2024).

⁸² „Verbindliche“ Entscheidung über die Zulässigkeit der Maßnahme seit BVerfG, Urteil v. 15.12.1970, 2 BvF 1/69, 2 BvR 629/68, 2 BvR 308/69 Rn. 77. Der Vorabkontrolleur muss seine Entscheidungsgründe außerdem protokollieren.

Demgegenüber hat sich das Gericht zu denkbaren Kontrollergesultenfolgen der Datenschutzkontrollinstanz nicht im Detail geäußert, ihr müssten jedoch „wirksame Befugnisse“ zustehen⁸³. Im Urteil zur strategischen Auslands-Fernmeldeaufklärung vom 5. Mai 2020 schreibt das Gericht, dass bei der administrativen Kontrolle im Bereich der strategischen Überwachung ein Beanstandungsrecht⁸⁴ „ausreichend“ sei.⁸⁵ Man könnte ob der detaillierteren Voraussetzungen bei der strategischen Überwachung⁸⁶ zu dem Schluss kommen, die „wirksamen Befugnisse“ außerhalb dieser Maßnahme so auszulegen, dass damit maximal eine Beanstandung gemeint sein kann, wenn diese bei der eingriffsintensiven strategischen Überwachung als ausreichend erachtet wurde. Dagegen spricht jedoch, dass der Datenschutzkontrollleur bei der strategischen Überwachung mit der gerichtsähnlichen Kontrollinstanz kooperieren soll und eine verbindliche Entscheidung durch sie herbeiführen kann. Zöge man demnach zur Auslegung des Begriffs der „wirksamen Befugnisse“ die zitierte Aussage des Gerichts heran, wonach ein Beanstandungsrecht „ausreichend“ sei, würde man sie aus ihrem Zusammenhang reißen, in welchem dezidiert ein Kooperationsmechanismus beschrieben wurde.

Auch hier stellt sich die Frage, ob es einen Mindestbestand an Befugnissen gibt, um noch von „Wirksamkeit“ der Kontrollergesultenfolgen ausgehen zu können. Einen konkreten Mindestbestand von Befugnissen hat das Bundesverfassungsgericht zwar nicht definiert. Weil es „wirksame Befugnisse“ fordert, sind jedoch zwingend Befugnisse vorzusehen. Wirksam bedeutet „eine beabsichtigte Wirkung erzielend“ oder „mit Erfolg wirkend“. Eine Kontrollergesultenfolge ist wirksam, wenn der rechtswidrige Zustand beendet wird.⁸⁷

Das ist bei der Beanstandung nur der Fall, wenn der Kontrollierte ihr Folge leistet. Der Kontrollleur kann dies jedoch nicht erzwingen. Die Beanstandung ist demnach nicht zwingend erfolgreich und nicht immer „wirksam“. Mit Sicherheit wird das Ergebnis daher nur erzielt, wenn der Kontrollleur zu einer abschließenden Entscheidung

⁸³ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 214 f.; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 141; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

⁸⁴ Nach deutschem Recht (außerhalb des Anwendungsbereichs des Unionsrechts) ist die Beanstandung der letzte Schritt einer Datenschutzkontrolle, ihr kommt keine Regelungswirkung zu, weshalb es sich nicht um einen Verwaltungsakt handelt. Sie dient nicht der Rechtsdurchsetzung, sondern als politisches Druckmittel, vgl. Schenke/Graulich/Ruthig/*Ruthig*, § 69 BKAG Rn. 12. Durch die Beanstandung wird ein „eingehendes Prüfverfahren“ ausgelöst: Die Aufsichtsbehörde, gegenüber der die Beanstandung ausgesprochen wird, muss dazu Stellung nehmen und kann entweder Maßnahmen ergreifen, um der Beanstandung abzuhefen oder sie „zurückweisen“, *Schulze/Bange*, ZD 2019, 199, 200 f. Im Anwendungsbereich der RL (EG) 2016/680 ist jedoch vorgeschrieben, dass die Befugnisse der Datenschutzbehörde „wirksam“ sind, weshalb hier eine Regelungswirkung vorauszusetzen ist.

⁸⁵ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276.

⁸⁶ Vgl. [Teil 2 A. III. 1. b. hh](#).

⁸⁷ So auch *Geiger*, DVBl 1990, 748, 751.

berechtigt ist, an die der Kontrollierte gebunden ist. Dafür spricht auch der Zweck der Rechtskontrolle von Nachrichtendiensten, der darin besteht, dass das durch die heimliche Vorgehensweise entstehende Rechtsschutzdefizit ausgeglichen werden soll.⁸⁸ Dieser Zweck wird nur erfüllt, wenn die Kontrollen bei einer festgestellten Rechtswidrigkeit Konsequenzen haben und die Kontrollerggebnisfolge verbindlich wirkt. Alternativ könnte dem Kontrolleur das Recht verliehen werden, sich bei Missachtung seiner Beauftragung an ein Gericht zu wenden, das abschließend entscheidet. Auch auf diese Weise ließe sich Verbindlichkeit herstellen.

ii) Fachkompetenz und Ressourcen

Das Bundesverfassungsgericht äußert sich darüber hinaus wiederholt zur *Fachkompetenz* und zu den *Ressourcen* der Kontrolleure. Die Vorabkontrollinstanz müsse über die „notwendige Sach- und Rechtskunde“ verfügen⁸⁹ und personell und sachlich⁹⁰ so ausgestattet sein, dass sie ihre Aufgabe „effektiv wahrnehmen“ könne⁹¹.

Die Datenschutzaufsichtsbehörden seien (personell) so auszustatten, dass ihnen regelmäßige Kontrollen möglich seien.⁹²

jj) Kontrollgegenstand- und tiefe

Die Vorabkontrolle erfolgt laufend und bei jeder Maßnahme.⁹³ In seinem Urteil zur Online-Durchsuchung schreibt das Bundesverfassungsgericht, der Kontrolleur müsse die Rechtmäßigkeit der Maßnahmen „eingehend“ prüfen.⁹⁴

Die Datenschutzkontrolle ist grundsätzlich zur Verhältnismäßigkeit jeder einzelnen Datenverarbeitung notwendig. Gleichzeitig erachtet das Bundesverfassungsgericht

⁸⁸ Vgl. [Teil 2 A. I. 3. a.](#)

⁸⁹ Zur Art. 10-Kontrolle: BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 - Rn. 77; außerhalb des Anwendungsbereichs von Art. 10 GG BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 118 („sachliche und personelle Voraussetzungen“); BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 215, so würden die Kontrolleure in die Lage versetzt, sich „eigenverantwortlich ein Urteil darüber zu bilden, ob die beantragte heimliche Überwachungsmaßnahme den gesetzlichen Voraussetzungen entspricht“.

⁹⁰ In BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 117 heißt es, es müssten die „sachlichen und personellen“ Voraussetzungen geschaffen werden.

⁹¹ Zur Art. 10-Kontrolle: BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 304, auch in der Landesverwaltung müsse eine „ausreichende Kontrolle“ existieren, soweit Daten aus Fernmeldeüberwachungen dorthin übermittelt werden; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 288.

⁹² BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 217; BVerfG, Urteil v. 20.4.2016, 1 BvR 966/09, 1 BvR 1140/09 Rn. 141.

⁹³ Jede eingriffsintensive Überwachungsmaßnahme bedarf der vorherigen Kontrolle, vgl. BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214.

⁹⁴ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259.

Stichprobenkontrollen in einem Kontrollintervall von bis zu zwei Jahren als ausreichend.⁹⁵

Das bedeutet, dass – anders als bei der Vorabkontrolle – nicht jede Datenverarbeitung tatsächlich zu kontrollieren ist.

Im Anwendungsbereich von Art. 10 GG sei die Kontrolle nur „wirksam“, wenn sie sich „auf alle Schritte des Prozesses der Fernmeldeüberwachung“ erstrecke, das heißt sowohl die Erfassung als auch die Verwertung der Daten umfasse.⁹⁶ Damit stellt das Gericht klar, dass die Datenschutzkontrolle auch im Anwendungsbereich von Art. 10 GG nicht von vornherein auf bestimmte Datenverarbeitungen beschränkt sein darf, sodass beispielsweise nur Datenerhebungen, nicht aber Datenübermittlungen kontrolliert werden können.

kk) Kontrollniveau

Im Zusammenhang mit der länderübergreifenden Antiterrordatei (vgl. § 1 ATDG) die eine informationelle Zusammenarbeit unterschiedlichster Behörden zur Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland ermöglicht, urteilte das Bundesverfassungsgericht, dass die Datenschutzkontrolleure von Bund und Ländern ebenfalls zusammenarbeiten und sich unterstützen dürfen.⁹⁷

Außerdem sei für eine effektive Aufsicht notwendig, so das Bundesverfassungsgericht im April 2022, dass die „kontrollierende Stelle jedenfalls alle Überwachungsmaßnahmen, denen eine Person durch eine Behörde ausgesetzt ist, in den Blick nehmen kann“. Das „Ausmaß“ und die „Rechtmäßigkeit“ eines Eingriffs und die damit verbundenen additiven Eingriffe ließen sich nicht „tragfähig beurteilen“, wenn die Aufsichtsbehörde nur auf einen beschränkten Datenbestand zugreifen könne.⁹⁸

Soweit das Gericht urteilt, dass die Aufsichtsbehörde für eine effektive Kontrolle alle Maßnahmen, denen eine Person ausgesetzt ist, in den Blick nehmen können muss, steht dies im Widerspruch zu der normierten abschließenden Kompetenz der bayerischen G 10-Kommission für alle Maßnahmen, die in Art. 10 GG eingreifen (Art. 28 BayVSG i. V. m. Art. 15 Abs. 2 Nr. 2 BayDSG). Nach geltendem Recht erstreckt sich die aufsichtliche Kontrolle in Bayern nur auf Maßnahmen außerhalb des Anwendungsbereichs von Art. 10 GG. Das Bundesverfassungsgericht geht auf diese erstmalig formulierten Anforderungen im Rahmen der Auseinandersetzung mit den jeweiligen Normen jedoch nicht mehr ein, weil die Beschwerdeführer sie im Laufe des Verfahrens

⁹⁵ BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83 - Rn. 155.

⁹⁶ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 171.

⁹⁷ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 216, *Sosna*, GSZ 2022, 245, 246.

⁹⁸ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

für erledigt erklärt hatten. So lässt sich aus dem Urteil nicht eindeutig ableiten, dass der bayerische Gesetzgeber Art. 28 BayVSG i. V. m. Art. 15 Abs. 2 Nr. 2 BayDSG anpassen müsste. Über den konkreten bayerischen Einzelfall hinaus ergibt sich aus der Formulierung, dass einfach-gesetzliche Regelungen, die im Anwendungsbereich von Art. 10 GG der Datenschutzaufsicht durch die gleiche Institution wie im Anwendungsbereich des RaiS keine Kenntnis von den Datenverarbeitungen ermöglichen, verfassungswidrig sind.

II) Barrieren

Hinsichtlich denkbarer Kontrollbarrieren fordert das Bundesverfassungsgericht, die Kontrolleure mit ausreichend Personal und Sachmitteln auszustatten. Insoweit begegnet es möglichen *Ressourcenbarrieren*.

Zudem äußert sich das Bundesverfassungsgericht zur Third Party Rule als *rechtlicher Barriere*.⁹⁹ Bei der Third Party Rule handelt es sich um eine unverbindliche Vereinbarung zwischen den Nachrichtendiensten¹⁰⁰, die im Einzelfall oder „allgemein für den laufenden Informationsaustausch“ getroffen wird¹⁰¹. Demnach dürfen Informationen, die ein Nachrichtendienst übermittelt hat, nicht ohne dessen Zustimmung an Dritte weitergegeben werden.¹⁰² Damit verfügt der übermittelnde Staat über eine Art „Informationsbeherrschungsrecht“, durch das er die Weiterverwendung durch den Empfänger bestimmen kann.¹⁰³ Als Dritte gelten in diesem Zusammenhang beispielsweise auch andere Behörden und Gerichte des Empfängerstaates.¹⁰⁴

Das Bundesverfassungsgericht betont, dass die Third Party Rule die Kontrolle nicht einschränken dürfe. Vielmehr sei davon auszugehen, dass sie durch eine die Geheimhaltung wahrende Kontrollkonstruktion und durch Absprachen mit den ausländischen Nachrichtendiensten nicht verletzt würde.¹⁰⁵

⁹⁹ Bezogen auf die Vorabkontrolle BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 224.

¹⁰⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 293; über die Rechtsnatur herrscht aber international keine Einigkeit, *Dietrich*, GSZ 2020, 174, 181.

¹⁰¹ *Gärditz*, DVBl 2015, 903, 904.

¹⁰² *Dietrich*, GSZ 2020, 173, 181; *Gazeas*, Übermittlung, S. 373.

¹⁰³ *Gärditz*, DVBl 2015, 903, 904.

¹⁰⁴ *Gärditz*, DVBl 2015, 903, 904.

¹⁰⁵ Bezogen auf die Vorabkontrolle BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 224 m. Verweis auf BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 292 ff.; BVerfG, Beschluss v. 12.10.2016 - 2 BVE 2/15 - Rn. 163 ff.; zur Datenschutzkontrolle nachrichtendienstlicher Maßnahmen außerhalb der strategischen Ausland-Fernmeldeaufklärung fehlt eine verfassungsgerichtliche Klarstellung noch. Wenn die Third Party Rule Kontrollen im Bereich der strategischen Ausland-Fernmeldeaufklärung nicht entgegengehalten werden kann, muss dies jedoch für vergleichbar eingriffsintensive Maßnahmen ebenso gelten.

b. Sonderfall strategische Ausland-Fernmeldeüberwachung

Für die Befugnis zur strategischen Ausland-Fernmeldeüberwachung durch den BND gelten zusätzliche, konkretisierte Anforderungen¹⁰⁶, die das Bundesverfassungsgericht in seinem Grundsatzurteil vom 5. Mai 2020 formuliert hat. Die verfassungsrechtlichen Vorgaben an die objektiv-rechtliche Kontrolle seien aus zwei Gründen besonders streng: Erstens müsse das Rechtsschutzdefizit ausgeglichen werden, das entstehe, weil der Gesetzgeber bezüglich von Ausländern im Ausland auf eine Benachrichtigungspflicht verzichten darf, um unter anderem die Tätigkeit des BND in diesem Land nicht zu offenbaren und womöglich Quellen zu gefährden. Zweitens solle dadurch die lediglich finale Anleitung der Überwachungsbefugnisse, das heißt, die Eingrenzung der Befugnis nur durch den Zweck ohne eingrenzende Tatbestandsvoraussetzungen durch „verfahrensmäßige Strukturierung“ ausgeglichen werden. Die Kontrolle böte ein „Gegengewicht“ zu den weiten Spielräumen des BND und gewährleiste, dass die Befugnisse im Rahmen der gesetzlichen Ziele eingesetzt würden.¹⁰⁷

Das Bundesverfassungsgericht konkretisiert, dass zwei Arten von Kontrolle normiert werden müssen: eine gerichtsähnliche und eine administrative Kontrolle.¹⁰⁸

aa) Kontrollmaßstab

Der Kontrollmaßstab ist die Rechtmäßigkeit der nachrichtendienstlichen Maßnahme.¹⁰⁹

bb) Zeitpunkt

Ob die gerichtsähnliche Kontrolle, die sich auf die „wesentlichen Verfahrensschritte“ und die damit verbundene Datenverarbeitung erstrecken muss, ex ante oder ex post erfolgt, liegt grundsätzlich im Entscheidungsspielraum des Gesetzgebers. Bei „grundlegenden“ Entscheidungen sei allerdings eine Vorabkontrolle geboten.¹¹⁰

¹⁰⁶ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 141. Bei der Formulierung der Kontrollvorgaben bezieht sich das Bundesverfassungsgericht jedoch nur auf die „strategische Überwachung“, was dafür spricht, dass diese Anforderungen nicht nur für die strategische Ausland-Fernmeldeüberwachung nach dem BNDG, sondern auch für die Überwachungen nach G 10 gelten, so auch *Alt*, Kompensatorische Kontrolle, S. 246.

¹⁰⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 266- 270, 273.

¹⁰⁸ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 274, dies müsse „organisationsrechtlich erkennbar sein“.

¹⁰⁹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 279.

¹¹⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 275, 278.

In seinem später ergangenen Urteil zum Bayerischen Verfassungsschutzgesetz zitiert das Bundesverfassungsgericht die entsprechende Randnummer seiner Entscheidung zur strategischen Ausland-Fernmeldeaufklärung im Zusammenhang mit der Feststellung, dass der Verhältnismäßigkeitsgrundsatz bei eingriffsintensiven Maßnahmen grundsätzlich eine vorherige Kontrolle durch eine unabhängige Stelle gebiete.¹¹¹ Dies spricht dafür, die „grundlegenden Entscheidungen“ so zu verstehen, dass zumindest die Genehmigung einer konkreten Anordnung zur strategischen Ausland-Fernmeldeüberwachung davon erfasst ist. Andererseits fordert das Gericht gerichtsähnliche ex ante-Kontrollen explizit unter anderem bei Datenübermittlungen oder bei Maßnahmen, die besondere Vertrauensbeziehungen berühren können; vergleichbare Formulierungen enthält das Urteil an anderen Stellen nicht.¹¹² Dies spricht dafür, dass das Bundesverfassungsgericht die Entscheidung darüber, welche Aspekte der strategischen Ausland-Fernmeldeüberwachung einer ex ante-Kontrolle unterliegen müssen, grundsätzlich dem Beurteilungsspielraum des Gesetzgebers überlassen wollte.

Der administrative Kontrolleur soll die Rechtmäßigkeit des gesamten Überwachungsprozesses während als auch nach den Datenverarbeitungen überprüfen.¹¹³

cc) Kontrolleur

Welche Institution die beiden Kontrollfunktionen übernehmen soll, liegt im Beurteilungsspielraum des Gesetzgebers. So könne die administrative Kontrolle bzw. die Datenschutzkontrolle entweder vom BfDI oder einer „verselbstständigte[n] Kontrollinstanz“ ausgeführt werden; in diesem Zusammenhang müsse der Gesetzgeber jedoch sicherstellen, dass die Third Party Rule die Kontrollen nicht „behinder[e]“. Es sei dem Gesetzgeber überlassen, ob die gerichtsähnliche und administrative Kontrolle „institutionell unter einem Dach zusammengefasst werden“, also integriert sind, oder ob sie voneinander unabhängig sind; davon abgesehen sei es aber wichtig, dass die institutionellen Strukturen „klar“ sind.¹¹⁴

¹¹¹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 214 m. Verweis auf BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 278.

¹¹² BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 194, 240, 257, ebenso im Zusammenhang mit der Anwendung von Suchbegriffen, wenn Maßnahmen gegen bestimmte Personen gerichtet sind, Rn. 188.

¹¹³ Es ist kein spezieller Zeitraum vorgegeben worden, weshalb eine Kontrolle während der Durchführung nicht ausgeschlossen ist, vgl. BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276.

¹¹⁴ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 282.

dd) Distanz

Das gerichtsähnliche Kontrolle müsse in „richterähnlicher Unabhängigkeit“ ausgestaltet sein, seine Mitglieder seien „weisungsfrei“, das administrative Kontrollorgan solle ebenfalls „unabhängig“ sein.¹¹⁵ Beide Kontrollen sollen in „institutioneller Eigenständigkeit“ erfolgen.¹¹⁶

Die Kontrolleure müssten „wirksam“ von Einflussnahmen „abgeschirmt“ werden und „vollständig unabhängig“ sein.¹¹⁷

ee) Modalitäten

Für die Vorabkontrolle gibt das Bundesverfassungsgericht unterschiedliche Modalitäten vor: teilweise muss sie in jedem Einzelfall erfolgen¹¹⁸ und teilweise kann sie „gegebenfalls in Zusammenarbeit mit der administrativen Kontrollinstanz“ „stichprobenmäßig“ erfolgen.¹¹⁹

Das administrative Kontrollorgan müsse den gesamten Prozess der strategischen Überwachung in Eigeninitiative stichprobenartig auf dessen Rechtmäßigkeit hin überprüfen können.¹²⁰ Dass die Stichprobenkontrollen mindestens alle zwei Jahre stattfinden sollen, fordert das Bundesverfassungsgericht allerdings nicht.¹²¹ Vielmehr soll die Stichprobenkontrolle bei der strategischen Ausland-Fernmeldeüberwachung einer ständig ausschließlich damit befassten Kontrollinstitution übertragen werden. Diese stichprobenartige Kontrolle erfolgt nicht nur punktuell (im Jahresrhythmus), sondern durchgehend.¹²²

ff) Initiative

Zur Kontrollinitiative bei der gerichtsähnlichen Kontrolle äußert sich das Bundesverfassungsgericht nicht. Sowohl hier wie auch außerhalb des Anwendungsbereichs der

¹¹⁵ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 275, 286.

¹¹⁶ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 281.

¹¹⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 281.

¹¹⁸ Dies betrifft „grundlegende Entscheidungen“, vgl. hierzu [Teil 2 A. III. 1. b. bb\).](#)

¹¹⁹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 278.

¹²⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276.

¹²¹ Vgl. [Teil 2 A. III. 1. a. ee\).](#)

¹²² „Zu gewährleisten ist eine kontinuierliche Kontrolle (...)“, BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 281.

strategischen Ausland-Fernmeldeüberwachung steht dem Kontrollierten bei der Genehmigung eingriffsintensiver Maßnahmen das Initiativrecht zu, weil er die genehmigungspflichtige Anordnung zunächst vorlegen muss¹²³.

Der Gesetzgeber solle jedoch prüfen, ob potenziell von Überwachungsmaßnahmen Betroffene das Recht haben sollten, die gerichtsähnliche Kontrolle anzustoßen und in diesem Prozess mit Verfahrensrechten ausgestattet zu sein.¹²⁴

Der administrative Kontrolleur soll eigeninitiativ tätig werden.¹²⁵ Er muss zudem die gerichtsähnliche Instanz zur Klärung von „grundlegenden Rechtsfragen“ konsultieren können.¹²⁶

gg) Kontrollmittel zur Informationsgewinnung

Die Kontrollinstanzen seien mit wirksamen Befugnissen auszustatten: Sie müssten „umfassend“ Zugriff auf alle Unterlagen haben, Auskünfte erteilt bekommen und Einsicht in Unterlagen und Daten sowie Informationen zu den verwendeten Programmen gewährt bekommen. Der BND habe ihnen „jederzeit Zutritt zu Diensträumen“ zu gestatten. Soweit das Verfahren und die Methodik nicht normiert seien, müsse beides den Kontrolleuren überlassen werden.¹²⁷

Das Gericht betont, dass die verschiedenen Schritte der Datenverarbeitung protokolliert werden müssten. Im Zweifel sei dies „im Benehmen“ von Kontrolleur und BND zu konkretisieren.¹²⁸

hh) Kontrollergebnisfolgen

Der gerichtsähnliche Kontrolleur soll „abschließend mit Wirkung für Bundesregierung und Nachrichtendienst“ entscheiden und „mindestens ebenso wirkungsvoll“ wie eine gerichtliche Kontrolle sein.¹²⁹

Im Gegensatz zur gerichtsähnlichen Kontrolle bedürfe die administrative Kontrolle keiner abschließenden Entscheidungskompetenz, ausreichend sei diesbezüglich ein Be-
anstandungsrecht. Die administrative Kontrollinstanz müsse die gerichtsähnliche Instanz allerdings zur Klärung von „grundlegenden Rechtsfragen“ konsultieren können¹³⁰, die ihrerseits verbindliche Entscheidungen treffen kann.

¹²³ Vgl. [Teil 2 A. III. 1. a. ff.](#)

¹²⁴ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 280, dieses Verfahren könne als In-Camera-Verfahren ausgestaltet sein.

¹²⁵ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - 1 BvR 2835/17 Rn. 276.

¹²⁶ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276.

¹²⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 289 f.

¹²⁸ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 291.

¹²⁹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 275.

¹³⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276.

Bei strukturellen Problemen und unüberbrückbaren Differenzen mit dem BND müssten die Kontrolleure gegenüber der Leitung des BND oder dem Bundeskanzleramt Beanstandungen aussprechen können, diese hätten sich dazu „gegebenenfalls“ zu verhalten.¹³¹

ii) Fachkompetenz und Ressourcen

Die Kontrollinstanzen müssten „personell kompetent und professionell ausgestattet sowie ausgewogen“ besetzt werden. Es müsse normativ vorgegeben sein, dass nur Personen ernannt werden, die „fachlich besonders [dafür] ausgewiesen und geeignet sind“, die inneren Strukturen und Abläufe des BND zu „durchdringen“. Insbesondere bei der administrativen Kontrolle müssten deshalb Personen mit „informationstechnischen Kenntnissen eingebunden sein“.¹³²

Die Mitglieder der gerichtsähnlichen Kontrollinstanz müssten „weisungsfrei und auf hinreichend lange und bestimmte Zeit fest berufen sein“. Bei der Besetzung müsse der „richterlichen Perspektive ein maßgebliches Gewicht“ beigemessen werden, weshalb eine „maßgebliche Zahl“ der Stellen mit langjährig erfahrenen Richtern zu besetzen sei. Zusätzlich könne auch Fachwissen aus anderen juristischen Berufen und technischer Sachverstand nützlich sein. Um dies zu erreichen, könne der Gesetzgeber Nichtjuristen als Gremienmitglieder vorsehen oder andere Optionen eröffnen, um die technische Expertise einzubinden.¹³³

Beiden Kontrollinstanzen müssten ausreichend Stellen und Mittel zur Verfügung gestellt werden. Dazu gehöre ein eigenes Budget und die Personalhoheit für alle Mitarbeiter (außer den Mitgliedern des gerichtsähnlichen Spruchkörpers und der Leitungsebene, die ernannt werden). Für die Wirksamkeit der gerichtsähnlichen Kontrolle sei es wichtig, so viele Stellen und Spruchkörper zu finanzieren, dass sie ihrem Kontrollauftrag sorgfältig nachkommen und qualifizierte Mitarbeiter gewinnen könne. Die finanziellen Mittel der administrativen Kontrolle müssten so umfangreich sein, dass die Filterung zum Aussondern von Inländerdaten und zum Schutz von Vertraulichkeitsbeziehungen kontrolliert werden könne, wofür gegebenenfalls eigene Software entwickelt werden müsse. Insgesamt müsste das Personal- und Mittelbudget mindestens dem des Ständigen Bevollmächtigten beim PKGr entsprechen.¹³⁴

¹³¹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 297.

¹³² BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 284 f.

¹³³ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 287.

¹³⁴ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 288.

jj) Kontrollgegenstand- und tiefe

Die Kontrolle des gerichtsähnlichen Kontrolleurs soll sich auf die „wesentlichen Verfahrensschritte“ der strategischen Überwachung sowie die damit verbundenen Datenverarbeitungen erstrecken.

Als wesentliche Verfahrensschritte gelten „die formalisierte Festlegung der verschiedenen Überwachungsmaßnahmen, auch im Bereich der Kooperationen, die konkreten Netzanordnungen, der Einsatz von Suchbegriffen, soweit diese gezielt auf Personen gerichtet sind, welche als mögliche Gefahrenquelle im unmittelbaren Interesse des Nachrichtendienstes stehen, der Einsatz von Suchbegriffen, die gezielt auf Personen gerichtet sind, deren Kommunikation einen besonderen Vertraulichkeitsschutz genießt, die zum Schutz solcher Vertraulichkeitsbeziehungen erforderlichen Abwägungsentscheidungen, der Umgang mit Daten, die möglicherweise dem Kernbereich privater Lebensgestaltung unterfallen, besonders kontrollbedürftige Übermittlungen, vor allem an ausländische Stellen, sowie die Voraussetzungen für die Festlegung einer Zusammenarbeit zur automatisierten Übermittlung von Verkehrsdaten zur bevorratenden Speicherung und Auswertung an ausländische Dienste“. Darüber hinaus erstreckte sich die gerichtsähnliche Kontrolle auf „die Nutzung von Daten unter Berufung auf besondere Gefahrensituationen, obwohl es sich um – erst in der manuellen Auswertung erkannte – Daten aus Telekommunikation unter Beteiligung von Deutschen oder Inländern handelt oder die Daten aus Überwachungsmaßnahmen stammen, die sich nicht auf Zwecke der Gefahrenfrüherkennung stützten, sondern unabhängig davon allein zur politischen Information der Bundesregierung angeordnet waren“.¹³⁵

Die administrative Rechtskontrolle soll ebenfalls den „gesamten Prozess der strategischen Überwachung“ auf seine Rechtmäßigkeit hin überprüfen. Dazu gehören „sowohl Einzelentscheidungen und Verfahrensabläufe als auch die Gestaltung der Datenverarbeitung und der Filterprozesse sowie der hierfür verwendeten technischen Hilfsmittel“.¹³⁶

kk) Kontrollniveau

Das „Gebot einer wirksamen und kohärenten Kontrolle“ fordere, dass zwischen den beiden Kontrolleuren ein offener und unmittelbarer Austausch gewährleistet werde. Der Austausch mit dem PKGr könne hingegen begrenzt werden, weil dessen Kontrolle anders strukturiert sei¹³⁷. Trotzdem seien regelmäßige Berichterstattungen gegenüber

¹³⁵ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 278, 281.

¹³⁶ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276.

¹³⁷ Vgl. [Teil 1 A. I. 2.](#)

dem PKGr vorzusehen und es müsse die Möglichkeit bestehen, dass die Kontrolleure ihre Kritik dem Parlament (und damit der Öffentlichkeit) mitteilen können.¹³⁸

Das Bundesverfassungsgericht äußert sich zudem zu möglichen Reibungsverlusten durch mehrere Kontrollinstanzen. Es müsse sichergestellt sein, dass der gesamte Prozess der strategischen Überwachung mitsamt der Datenverarbeitung und -übermittlung „potenziell umfassend“ der Rechtmäßigkeitskontrolle unterliege. Wenn eine gerichtsähnliche Kontrolle nicht vorgesehen sei, müsse wenigstens eine administrative Kontrolle möglich sein.¹³⁹

ll) Barrieren

Gegenüber den unabhängigen, auf Geheimhaltung verpflichteten Kontrollinstanzen können sich der BND und die Bundesregierung nicht auf die „Third Party Rule“ berufen. Die gesetzliche Regelung müsse sicherstellen, dass die Kontrollinstanzen organisatorisch so ausgestaltet würden, dass diese nicht als „Dritte“ wahrgenommen werden. Da es sich bei den Vereinbarungen um „flexible Verwaltungspraktik“ handele, könnten die Absprachen zukünftig dahingehend angepasst werden. Andererseits müsse die für die Wahrung außen- und sicherheitspolitischer Interessen „bedeutsame“ Kooperation mit anderen Nachrichtendiensten fortgeführt werden können. Dass dies grundsätzlich möglich sei, zeige das Beispiel von Großbritannien, wo die „Third Party Rule“ in einem vergleichbaren Kontrolldesign keine Probleme bereite.¹⁴⁰

Daneben formuliert das Bundesverfassungsgericht konkrete Anforderungen, um *Ressourcenbarrieren* zu vermeiden. Demnach seien für beide Kontrollmodi „hinreichendes Personal und hinreichende Mittel bereitzustellen“.¹⁴¹

mm) Fazit

Obwohl die Vorgaben an die Rechtskontrolle der strategischen Ausland-Fernmeldeüberwachung in ihrer dualen Struktur den Maßgaben gegenüber sonstigen eingriffsintensiven nachrichtendienstlichen Mitteln entsprechen¹⁴², bestehen im Detail weitreichende Unterschiede. Insgesamt hat das Bundesverfassungsgericht die Rechtskontrolle

¹³⁸ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 297.

¹³⁹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 279.

¹⁴⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 293 ff.

¹⁴¹ Vgl. zu den Anforderungen im Detail, [Teil 2 A. III. 1. b. ii\)](#); BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 288.

¹⁴² Das Bundesverfassungsgericht hätte die „Anforderungen an unabhängige Kontrollstrukturen für heimliche Überwachungsmaßnahmen von BND und Verfassungsschutz in der Sache parallel formuliert“, Gärditz, GSZ 2022, 161, 170; vgl. auch Ogorek, NJW 2022, 1570, 1572; vgl. [Teil 2 A. III. 1. a.](#)

der strategischen Ausland-Fernmeldeüberwachung detaillierter beschrieben. Die Unterschiede betreffen:

- die *Modalität der Datenschutzkontrollen*, wonach die Datenschutzkontrolle durchgehend stichprobenartig prüft anstatt nur mindestens alle zwei Jahre,
- die *Kontrollmittel zur Informationsgewinnung*, bei denen das Bundesverfassungsgericht bestimmte, notwendige Befugnisse der Kontrolleure explizit aufzählt,
- die *Kontrollergesultfolgen der Datenschutzkontrolle*, hinsichtlich derer das Bundesverfassungsgericht mindestens ein Beanstandungsrecht fordert, es allerdings zulässt, dass der administrative Kontrolleur bei „grundlegenden“ Rechtsfragen das gerichtsähnliche Organ konsultieren kann,
- die *Fachkompetenz und Ressourcen*, da ein eigenes Budget für den Kontrolleur, die Personalhoheit und die Einbindung technischer Expertise sowie die Besetzung einiger Stellen mit Personen, die eine langjährige richterliche Erfahrung vorweisen können, vorgeschrieben ist,
- die *Kontrolltiefe*, die vor allem bei der richterähnlichen Kontrolle eingehend beschrieben wird sowie das *Kontrollniveau*.

Zudem ist die gerichtsähnliche Kontrolle nicht auf die ex ante-Kontrolle beschränkt, sondern prüft ggf. darüberhinausgehend¹⁴³ „die wesentlichen Verfahrensschritte“ und die damit verbundene Datenverarbeitung.

2. Zweistufiges Kernbereichskonzept

Gegenüber den in das Raster des dualen Kontrollkonzepts einordbaren Kontrollvorgaben nimmt die in einigen Entscheidungen beschriebene Kernbereichskontrolle¹⁴⁴ eine Sonderrolle ein. Für solche Befugnisse, die „verletzungsgeneigt“ sind, wie beispielsweise die Wohnraumüberwachung, die Datenerhebung aus informationstechnischen Systemen, die (Quellen-)Telekommunikationsüberwachung sowie den Einsatz von Vertrauenspersonen und Verdeckten Mitarbeitern, muss der Gesetzgeber grundsätzlich spezifische Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung schaffen und dabei ein zweistufiges Schutzkonzept beachten.¹⁴⁵ Soweit die Erhebung von kern-

¹⁴³ Nur für „grundlegende Fragen“ ist eine Vorabkontrolle unabdingbar.

¹⁴⁴ U.a. in BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 271 ff.; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 123, 129, 177, 200 f., 220, 224; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 278 ff., 305 ff., 315 ff.; BVerfG, Beschluss v. 9.12.2022 - 1 BvR 1345/21 - Rn. 108 ff.

¹⁴⁵ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 280 ff.; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 126; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 205 ff.; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 277 ff., 305 ff., 315 ff.; BVerfG, Beschluss v.

bereichsrelevanten Daten nicht (typischerweise) im Vorhinein bereits bei der Datenerhebung ausgeschlossen werden kann (Erhebungsebene), muss eine „unabhängige, nicht mit Sicherheitsaufgaben betraute“ Stelle der sicherheitsbehördlichen Auswertung vorgeschaltet sein, die darüber entscheidet, ob die Daten kernbereichsverletzend sind und deshalb gelöscht werden müssen (Auswertungs- und Verwertungsebene).¹⁴⁶

a. Grundsatz

Das Bundesverfassungsgericht hat im Rahmen seines Zwei-Stufen-Modells differenzierte Vorgaben für die Ausgestaltung des Kernbereichsschutzes formuliert.

Zunächst ist die zielgerichtete Erhebung von Kernbereichsdaten wegen des damit verbundenen Verstoßes gegen die Menschenwürde unzulässig.¹⁴⁷ Soweit die zufällige Erhebung von kernbereichsrelevanten Informationen bei verletzungsgeneigten Befugnissen nicht von vornherein ausgeschlossen werden kann und kernbereichsrelevante Daten daher möglicherweise verarbeitet werden, gelten abhängig vom Zeitpunkt der Kenntnisnahme unterschiedliche Anforderungen: Fällt die Kernbereichsrelevanz bereits bei der Erhebung auf, muss die Verarbeitung unterbrochen werden. Ist sie erst während der Auswertung erkennbar, müssen diese Daten gelöscht werden. Die Löschung ist zu protokollieren.¹⁴⁸

b. Einbindung einer unabhängigen Stelle

Auf der Auswertungs- und Verwertungsebene muss bei verletzungsgeneigten Befugnissen eine „unabhängige, nicht mit Sicherheitsaufgaben betraute“ Stelle eingebunden werden.¹⁴⁹ Diese Verfahrensregelung soll verhindern, dass die Sicherheitsbehörde von

9.12.2022 - 1 BvR 1345/21 - Rn. 108 ff.; *Dietrich*, Hdb. des Rechts der Nachrichtendienste, 1017, 1069; BL-AG- BVerfGE v. 26.4.2022 zum BayVSG, Anlage 4 (abgerufen am: 31.8.24), S. 17; kritisch *Löffelmann/Zöller*, Nachrichtendienstrecht, Rn. 102.

¹⁴⁶ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 282 f., wonach auch eine „automatische Sichtung“ nicht ausgeschlossen ist, soweit sie zukünftig technisch möglich werden sollte; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 224; *Schneider*, JuS 2021, 29, 33; für die Rechtsgrundlagen von Vertrauenspersonen und Verdeckten Mitarbeitern gilt, dass ein Sichtung durch eine unabhängige Stelle nicht zwingend notwendig ist, BVerfG, Beschluss v. 9.12.2022 - 1 BvR 1345/21 - Rn. 117 f.; BL-AG- BVerfGE v. 26.4.2022 zum BayVSG, Anlage 4 (abgerufen am: 31.8.24), S. 1, 3.

¹⁴⁷ Für die Wohnraumüberwachung gilt überdies die Besonderheit, dass eine Verletzung des Kernbereichs gesetzlich vermutet werden und das Gegenteil zunächst positiv festgestellt werden muss, BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 305.

¹⁴⁸ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 278 ff.; BVerfG, Beschluss v. 9.12.2022 - 1 BvR 1345/21 - Rn. 109; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 240; BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 283.

¹⁴⁹ Vgl. [Teil 2 A. III. 2.](#)

den kernbereichsverletzenden Informationen Kenntnis erlangt.¹⁵⁰ Die unabhängige Stelle soll diese Daten vorab herausfiltern und löschen.¹⁵¹

aa) Kontrollmaßstab

Bei der Wohnraumüberwachung und dem Eingriff in informationstechnische Systeme (Online-Durchsuchung) müssen die Ergebnisse der Überwachung zwingend durch eine unabhängige Stelle gesichtet werden. Nur für Situationen mit Gefahr in Verzug können Ausnahmen davon vorgesehen werden. Das Bundesverfassungsgericht hat entschieden, dass alle durch diese Maßnahmen gewonnenen Daten vollständig gesichtet werden müssen. Bei der Online-Durchsuchung können Bedienstete des Nachrichtendienstes bei der Sichtung eingebunden werden, wenn die unabhängige Stelle an technische und fachliche Grenzen stößt; das gilt jedenfalls, soweit die tatsächliche Durchführung und die Entscheidungsverantwortung „maßgeblich in der Verfassungsschutzbehörde gegenüber unabhängigen Händen“ bleibt.¹⁵²

bb) Flexible Vorgabe bei Telekommunikationsüberwachung und dem Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten

Beim Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern sowie bei der (Quellen-)Telekommunikationsüberwachung muss die Sichtung durch eine unabhängige Stelle nicht in jeder Fallkonstellation erfolgen.¹⁵³

Die Erforderlichkeit „einer solchen Sichtung hängt von der Art sowie gegebenenfalls auch der Ausgestaltung der jeweiligen Befugnis ab“, auf die Sichtung könne „umso eher verzichtet werden, je verlässlicher schon auf der ersten Stufe die Erfassung kernbereichsrelevanter Sachverhalte vermieden wird und umgekehrt“. Vertrauensleute sowie ihre Führer im Nachrichtendienst müssen prüfen, ob sie kernbereichsrelevante Informationen erhoben haben, die sie nicht weitergeben dürfen.¹⁵⁴ In Zweifelsfällen müsse zumindest der behördliche Datenschutzbeauftragte die Daten sichten.¹⁵⁵

¹⁵⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 286; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 220.

¹⁵¹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 286; BL-AG- BVerfGE v. 26.4.2022 zum BayVSG, Anlage 4 (abgerufen am: 31.8.24), S. 1, 3.

¹⁵² BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 278 ff; BVerfG, Beschluss v. 9.12.2022 - 1 BvR 1345/21 - Rn. 282, 286, 306, 315; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 224.

¹⁵³ BVerfG, Beschluss v. 9.12.2022 - 1 BvR 1345/21 - Rn. 117; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 Rn. 240.

¹⁵⁴ BVerfG, Beschluss v. 9.12.2022 - 1 BvR 1345/21 - Rn. 118.

¹⁵⁵ BVerfG, Beschluss v. 9.12.2022 - 1 BvR 1345/21 - Rn. Rn. 119.

3. Verfassungsrechtliche Herleitung der Kontrollmodi

Wie leitet das Bundesverfassungsgericht diese Kontrollvorgaben aus grundgesetzlichen Maßstäben und Rechtsfiguren ab? Zentral ist zunächst, dass die verfassungsrechtlichen Maßgaben an die Rechtskontrolle der Nachrichtendienste ausschließlich aus den einschlägigen Grundrechten¹⁵⁶ abgeleitet werden.

a. Art. 10 GG

In den früheren Entscheidungen des Bundesverfassungsgerichts zum Nachrichtendienstrecht wurde die Kontrolle überwiegend im Zusammenhang mit Art. 10 Abs. 2 S. 2 GG thematisiert.¹⁵⁷ Mit der Grundgesetzänderung von 1968 hat das Fernmeldegeheimnis im Nachrichtendienstrecht gegenüber den anderen Grundrechten eine herausgehobene Stellung erhalten. Fortan ermöglichte es der neu eingeführte Art. 10 Abs. 2 S. 2 GG, gesetzlich vorzusehen, dass der Betroffene unter bestimmten Voraussetzungen nicht benachrichtigt wird und somit keinen Rechtsschutz erlangen kann:

„Dient die Beschränkung [des Post- und Fernmeldegeheimnisses] dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.“¹⁵⁸

aa) Tatbestandsvoraussetzungen

Art. 10 Abs. 2 S. 2 GG knüpft das Absehen von der Benachrichtigungspflicht an bestimmte Bedingungen.

(1) Schutzgüter

Demnach darf die Benachrichtigungspflicht nur entfallen, wenn die Beschränkung dem Schutz der freiheitlichen demokratischen Grundordnung oder des Bestandes oder

¹⁵⁶ Vgl. [Teil 2 A. II.](#)

¹⁵⁷ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69; BVerfG, Beschluss v. 20.6.1984 - 1 BvR 1494/78; BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95.

¹⁵⁸ Siebzehntes Gesetz zur Ergänzung des Grundgesetzes v. 24.6.1968, [BGBl I S. 709 f.](#)

der Sicherung des Bundes oder eines Landes dient. Diese Schutzgüter sind eng auszulegen.¹⁵⁹ Für die Definition der „freiheitlich demokratischen Grundordnung“ ist die Rechtsprechung des Bundesverfassungsgerichts maßgeblich, die einfach-rechtlich in § 4 Abs. 2 BVerfSchG aufgegriffen wurde.¹⁶⁰ Davon erfasst sind zentrale Prinzipien, wie „die Achtung der Menschenrechte des Grundgesetzes, die Volkssouveränität, die Gewaltenteilung, die Gesetzmäßigkeit der Verwaltung und die Unabhängigkeit der Gerichte“. ¹⁶¹ Der Bestand meint die „elementarsten rechtlichen und sozialen Gegebenheiten“, also die Handlungsfähigkeit des Staates, die territoriale Integrität und das Staatsvolk.¹⁶²

(2) „Dienen“

Art. 10 Abs. 2 S. 2 GG setzt nicht voraus, dass diesen Schutzgütern eine „Gefahr“ droht.¹⁶³ Stattdessen reicht es aus, wenn die Beschränkung diesen Schutzgütern „dient“. Das bedeutet, die Beschränkungsnormen müssen den Zweck der Schutzgüter verfolgen.¹⁶⁴

Da die Schutzgüter eng auszulegen sind, können Maßnahmen zur Beobachtung der allgemeinen organisierten Kriminalität¹⁶⁵ ihnen richtigerweise nicht dienen.¹⁶⁶

Diesen verfassungsrechtlichen Anforderungen wird das G 10 nicht vollständig gerecht. Während der Gesetzgeber den Anwendungsbereich von Art. 10 Abs. 2 S. 2 GG bei § 13 G 10 beachtet, ist ihm dies bei § 12 Abs. 1 S. 2 G 10 nicht gelungen. § 13 G 10, der festlegt, dass der Rechtsweg bei Beschränkungsmaßnahmen nach den §§ 3 und 5 Abs. 1 S. 3 Nr. 1 G 10 vor ihrer Mitteilung an den Betroffenen ausgeschlossen ist, beschränkt den Ausschluss auf Maßnahmen, die von Art. 10 Abs. 2 S. 2 GG erfasst sind.

¹⁵⁹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 Rn. 271; Huber/Voßkuhle/Gusy, Art. 10 GG Rn. 98; Paeffgen, StV 1999, 668, 671.

¹⁶⁰ P. M. Huber/Voßkuhle. Andreas/Gusy, Art. 10 GG Rn. 98; vgl. [Teil 1 B. II. 3.](#)

¹⁶¹ Maßgeblich ist insoweit die frühere Definition des Bundesverfassungsgerichts, vgl. [Teil 1 B. II. 3.](#); Münch/Kunig/Martini, Art. 10 GG Rn. 150, m. weiteren Beispielen Huber/Voßkuhle/Gusy, Art. 10 GG Rn. 98.

¹⁶² Dürig/Herzog/Scholz/Durner, Art. 10 GG Rn. 216.

¹⁶³ Münch/Kunig/Martini, Art. 10 GG Rn. 154; Huber/Voßkuhle/Gusy, Art. 10 GG Rn. 98.

¹⁶⁴ Dürig/Herzog/Scholz/Durner, Art. 10 GG Rn. 220.

¹⁶⁵ Zum Begriff [Teil 1 B. II. 3. a. bb.](#), Paeffgen, StV 1999, 668, 671.

¹⁶⁶ So auch bezüglich der international organisierten Geldwäsche Dürig/Herzog/Scholz/Durner, Art. 10 GG Rn. 220. Explizit zur Beobachtung der organisierten Kriminalität ermächtigt ist der BND in § 5 Abs. 1 S. 3 Nr. 4-8 G 10 und die LfV in Bayern, Hessen und dem Saarland (Art. 3 S. 2 [BayVSG](#); § 2 Abs. 2 Nr. 5 [HVSg](#); § 3 Abs. 1 Nr. 4 [SVerfSchG](#)). Die Verfassungsschutzbehörden können Maßnahmen gem. § 3 G 10 zwar auch ggf. gegen Bestrebungen der organisierten Kriminalität richten, dies ist jedoch in der Norm selbst nicht angelegt. Die Normen adressieren Gefahren für den Bestand und die Sicherheit der BRD.

Auf andere Beschränkungen ist die Norm nicht anwendbar, auch nicht analog.¹⁶⁷ Demgegenüber regelt § 12 Abs. 1 S. 2 G 10 Fälle, in denen die Benachrichtigung Betroffener vorübergehend entfallen kann. Eine solche Benachrichtigung kann auch bei Beschränkungen gem. § 5 Abs. 1 S. 3 Nr. 8 G 10 entfallen (§ 12 Abs. 2, Abs. 1 S. 2 G 10). Gemäß dieser Norm ist die strategische Überwachung zur Sammlung von Informationen über die Gefahr „der unbefugten gewerbs- oder bandenmäßig organisierten Verbringung von Betäubungsmitteln in das Gebiet der Europäischen Union in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland“ zulässig. Der gewerbs- und bandenmäßige Betäubungsmittelhandel ist eine Erscheinungsform der organisierten Kriminalität und deshalb nicht von Art. 10 Abs. 2 S. 2 GG erfasst. Das bedeutet, dass der Ausschluss von der Benachrichtigungspflicht verfassungsrechtlich nicht auf Art. 10 Abs. 2 S. 2 GG gestützt werden kann. Im Urteil zur Telekommunikationsüberwachung nach dem G 10 vom 14. Juli 1999 hat das Bundesverfassungsgericht zwar entschieden, dass kriminelle Handlungen Gegenstand der strategischen Überwachung sein können, wenn sie ein „besonderes Gefahrenpotenzial für den Bestand und die Sicherheit der Bundesrepublik“ bergen¹⁶⁸; dazu, ob bei dieser Maßnahme vor dem Hintergrund der engen Formulierung in Art. 10 Abs. 2 S. 2 GG die Benachrichtigungspflicht ausgeschlossen sein darf, hat es sich damals nicht geäußert.

Mittlerweile hat dieses Problem keine praktische Bedeutung mehr: Erstens wurde die Möglichkeit zum vorübergehenden Absehen von der Mitteilungspflicht und der damit verbundene Eingriff in Art. 19 Abs. 4 GG für sämtliche nachrichtendienstliche Beobachtungsaufträge de facto als gerechtfertigt anerkannt.¹⁶⁹ Zweitens hat das Bundesverfassungsgericht bei heimlichen Maßnahmen den mit der fehlenden Benachrichtigung verbundenen (vorübergehenden) Wegfall des Rechtsweges als verfassungsgemäß gebilligt, soweit die aus der Verhältnismäßigkeit abgeleiteten Anforderungen an eine alternative Kontrolle gewahrt werden. Im Urteil zur strategischen Auslands-Fernmeldeaufklärung schreibt das Gericht, dass Art. 10 Abs. 2 S. 2 GG ihren (aus der Verhältnismäßigkeit hergeleiteten) Vorgaben zur Ausgestaltung der objektivrechtlichen Kontrolle nicht entgegenstehe, weil der Anwendungsbereich eng begrenzt sei.¹⁷⁰

¹⁶⁷ Dürig/Herzog/Scholz/Durner, Art. 10 GG Rn. 220; Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 3.

¹⁶⁸ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95; Bäcker, Beschwerdeschrift G 10, S. 40.

¹⁶⁹ In BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 271 schreibt das Gericht dazu: „Sieht das Gesetz Benachrichtigungspflichten nicht vor, kann Art. 10 Abs. 2 S. 2 GG zu beachten sein.“

¹⁷⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 271.

Im Ergebnis ist es daher weder für die Rechtsprechung noch für die Praxis von zentraler Bedeutung, dass der Anwendungsbereich von Art. 10 Abs. 2 S. 2 GG auf bestimmte Beobachtungsaufträge begrenzt ist, weil aus der Verhältnismäßigkeitsprüfung gleichläufige Anforderungen folgen.¹⁷¹

bb) Rechtsfolge: Nachprüfung

Bei Beschränkungen, die dem Schutz dieser Rechtsgüter dienen, liegt es im Ermessen des einfachen Gesetzgebers, festzulegen, dass die Benachrichtigungspflicht und der Rechtsweg entfallen.¹⁷² Wenn der Gesetzgeber eine solche Regelung erlässt, muss er eine „Nachprüfung durch Organe oder Hilfsorgane des Parlaments“ vorsehen. Deshalb ist der Bundestag oder das jeweilige Landesparlament verpflichtet, ein solches Organ oder Hilfsorgan zu schaffen.¹⁷³

Der Begriff der „Nachprüfung“ könnte so zu verstehen sein, dass es sich um eine nachträgliche Rechtmäßigkeitskontrolle handelt. Alternativ könnte der Begriff als Synonym für „Kontrolle“ gewählt worden sein.¹⁷⁴ In diesem Fall wäre damit kein bestimmter Kontrollzeitpunkt verbunden. Die Gesetzgebungsmaterialien enthalten keine Erläuterungen zum Begriff der „Nachprüfung“.¹⁷⁵ In der Literatur wird die Bedeutung des Begriffs nicht analysiert. Aus der Begründung zur Verfassungsänderung ergibt sich, dass dem Gesetzgeber „ein Regelungsermessen hinsichtlich des Verfahrens der Nachprüfung und Unterrichtung der Volksvertretung“ zustehen sollte.¹⁷⁶ Der Zeitpunkt ist ein wesentlicher Aspekt der Verfahrensgestaltung. Hätte der verfassungsändernde Gesetzgeber eine nachträgliche Kontrolle vorgeben wollen, hätte es dazu ob der Mehrdeutigkeit der Formulierung detaillierterer Ausführungen in der Gesetzesbegründung bedurft. So spricht der Regelungsspielraum dafür, dass der Begriff der „Nachprüfung“ synonym zu dem der „Kontrolle“ verwendet wurde. Diese Schlussfolgerung deckt sich mit der Umsetzung des einfachen Gesetzgebers und der parlamentarischen Praxis nach Einsetzung der G 10-Kommission. § 9 Abs. 2 G 10 a.F. ordnete an, dass der zuständige Minister die G 10-Kommission monatlich über die von ihm angeordneten

¹⁷¹ Vgl. [Teil 2 A. III. 3. d.](#)

¹⁷² Dürig/Herzog/Scholz/Durner, Art. 10 GG Rn. 223; Münch/Kunig/Martini, Art. 10 GG Rn. 156.

¹⁷³ Münch/Kunig/Martini, Art. 10 GG Rn. 158.

¹⁷⁴ <https://www.duden.de/rechtschreibung/Nachpruefung> (abgerufen am 31.8.2024).

¹⁷⁵ BT-Drs. 5/1879, Entwurf eines Gesetzes zur Ergänzung des Grundgesetzes v. 13.6.1967, S. 18.

¹⁷⁶ BT-Drs. 5/1879, Entwurf eines Gesetzes zur Ergänzung des Grundgesetzes v. 13.6.1967, S. 18.

Beschränkungsmaßnahmen unterrichtet und dass die Kommission über deren Zulässigkeit entscheidet.¹⁷⁷ Aus der Gesetzesbegründung ergibt sich, dass die Kontrolle laufend – und nicht erst nachträglich – erfolgt, denn bei ablehnender Entscheidung der Kommission hat der Minister dafür Sorge zu tragen, dass die auf Grund der Anordnung ergangene Maßnahme unverzüglich eingestellt wird.¹⁷⁸ Nach Abschluss der Beschränkung wäre eine Einstellung unmöglich. Bei der Änderung des G 10 im Jahr 1978 hat der zuständige Rechtsausschuss sich zudem erfolgreich dafür eingesetzt, dass § 9 Abs. 2 G 10 a.F. so angepasst wird, dass der Minister die G 10-Kommission bereits vor Vollzug der Anordnung unterrichtet, sodass die G 10-Kommission die Maßnahme vorab genehmigt.¹⁷⁹ Dabei handelte es sich um ein bereits praktiziertes Verfahren.¹⁸⁰ Das bedeutet, dass der einfache Gesetzgeber den Begriff der Nachprüfung als Kontrolle interpretiert hat, die nicht als nachträgliche Kontrolle intendiert war, sondern vorab und laufend erfolgt.

Im Ergebnis ist der Begriff der „Nachprüfung“ also synonym zu dem der „Kontrolle“ zu verstehen. Der verfassungsändernde Gesetzgeber wollte somit keinen bestimmten Kontrollzeitpunkt vorgeben, sondern hat die nähere Ausgestaltung der Kontrolle dem Gesetzgeber überlassen.

cc) Auslegung des Bundesverfassungsgerichts

Die Anforderungen an die „Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane“ hat das Bundesverfassungsgericht in mehreren Entscheidungen herausgearbeitet.¹⁸¹

(1) Erstes Abhörurteil

Das Bundesverfassungsgericht urteilte bereits 1970, dass die Grundgesetzänderung von Art. 10 GG und die Ergänzung von Art. 19 Abs. 4 GG um S. 3 mit der Ewigkeitsgarantie aus Art. 79 Abs. 3 GG vereinbar und damit verfassungskonform ist.¹⁸² Es entschied

¹⁷⁷ BT-Drs. 5/1880, Entwurf eines Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zur Artikel 10 Grundgesetz) (G 10) v. 13.6.1967, S. 3.

¹⁷⁸ BT-Drs. 5/1880, Entwurf eines Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zur Artikel 10 Grundgesetz) (G 10) v. 13.6.1967, S. 11.

¹⁷⁹ BT-Drs. 8/1848, Beschlußempfehlung und Bericht des Rechtsausschusses (6. Ausschuß) v. 1.6.1978, S. 8.

¹⁸⁰ BT-Drs. 8/1848, Beschlußempfehlung und Bericht des Rechtsausschusses (6. Ausschuß) v. 1.6.1978, S. 8.

¹⁸¹ Vgl. auch *Alt*, Kompensatorische Kontrolle, S. 80 ff.

¹⁸² BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69.

in diesem Zusammenhang auch über die Verfassungskonformität der einfach-rechtlichen Ausgestaltung im neu geschaffenen § 9 G 10. Das Urteil ist nur knapp (im Verhältnis von 5:3) zugunsten der Verfassungskonformität der Änderung ausgefallen und wurde auch in der Wissenschaft deutlich kritisiert.¹⁸³ Dennoch resümiert Gusy, das Urteile habe „langfristig eher befriedend“ gewirkt: Die „verfahrensrechtlichen Anforderungen an heimliche Grundrechtseingriffe“ seien seit dem Urteil „wesentlich deutlicher als zuvor“.¹⁸⁴

Bei ihrer Auslegung von Art. 10 Abs. 2 S. 2 GG fokussierte sich die Senatsmehrheit auf die Formulierung, wonach die Nachprüfung durch von der Volksvertretung bestellte Organe oder Hilfsorgane „an die Stelle des Rechtsweges“ tritt. Daraus schließen die Richter, der verfassungsändernde Gesetzgeber habe eine *Gleichwertigkeit* zwischen dem gerichtlichen Rechtsschutz und der alternativen Kontrollinstanz postuliert.¹⁸⁵ Anschließend konkretisieren sie diese „materiell[e] und verfahrensmäßig[e]“ Gleichwertigkeit zur gerichtlichen Kontrolle, indem sie Anforderungen an die Ausgestaltung der alternativen Kontrollinstanz formulieren: So müsse das vom Parlament bestellte Organ oder Hilfsorgan „mindestens ebenso wirkungsvoll“ sein, „auch wenn der Betroffene keine Gelegenheit [habe], in diesem ‚Ersatzverfahren‘ mitzuwirken.“ Die Kontrollinstitution müsse in „richterlicher Unabhängigkeit“ ausgestaltet sein und für alle an der Überwachung Beteiligten „verbindlich“ sowohl über die Zulässigkeit derselben als auch über die Benachrichtigung der Betroffenen entscheiden und die Maßnahme untersagen, „wenn es an den rechtlichen Voraussetzungen dazu fehlt“. Das Organ bzw. Hilfsorgan könne „innerhalb oder außerhalb des Parlaments“ gebildet werden, müsse jedoch über die „notwendige Sach- und Rechtskunde verfügen“ und „weisungsfrei“ sein. Seine Mitglieder seien auf bestimmte Zeit fest zu berufen. Es müsse „kompetent“ sein, alle Organe, die mit dem Eingriff in Art. 10 GG befasst sind, zu überwachen. Die Kontrolleure sollten „laufend“ kontrollieren und über Zugang zu allen für die Entscheidung „erheblichen Unterlagen des Falles“ verfügen. Die Kontrolle müsse „Rechtskontrolle“ sein. Zudem lasse Art. 10 Abs. 2 S. 2 GG eine gesetzliche Ausgestaltung zu, bei der das Organ aus Opportunitätsgründen die Anzahl der Überwachungsfälle sogar dann einschränken darf, wenn die gesetzlichen Voraussetzungen eingehalten worden sind.¹⁸⁶

Darüber hinaus betonen die Richter im Rahmen der Verhältnismäßigkeitsprüfung, dass Art. 10 Abs. 2 S. 2 GG für den Fall, dass eine Zweckgefährdung entfalle, fordere, den Betroffenen (nachträglich) zu benachrichtigen.¹⁸⁷ Die Norm eröffne zudem zwar

¹⁸³ Vgl. statt vieler z.B. Häberle, JZ 1971, 145.

¹⁸⁴ Huber/Voßkuhle/Gusy, Art. 10 GG Rn. 97.

¹⁸⁵ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 77.

¹⁸⁶ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 77.

¹⁸⁷ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 74.

die Möglichkeit, eine alternative Rechtskontrolle einzuführen, zwingt den Gesetzgeber aber nicht dazu.¹⁸⁸ Eingriffe in Art. 10 GG seien in diesem Zusammenhang nur zulässig, wenn „konkrete Umstände den Verdacht eines verfassungsfeindlichen Verhaltens rechtfertigen“ und der Eingriff in Art. 10 GG nur als ultima ratio angewandt würde.¹⁸⁹ Zudem sei die Überwachung auf die Personen zu beschränken, gegenüber denen ein solcher Verdacht bestünde; gleichwohl könnten auch Nachrichtenverbindungen von dritten Personen dann überwacht werden, wenn angenommen werden kann, dass sie für die Zwecke des „Verdächtigen“ benutzt werden.¹⁹⁰

(2) Zweite Abhörentscheidung

Während das Bundesverfassungsgericht in seiner ersten Abhörentscheidung mit der Verfassungsmäßigkeit der Grundgesetzänderungen in Art. 10 und 19 GG und mit der Individualbeschränkung nach dem G 10 befasst war, galt es in der zweiten Abhörentscheidung 1984, die Verfassungsmäßigkeit der strategischen Überwachung nach G 10 (§ 3 G 10 a.F.) zu beurteilen.¹⁹¹ Zur Kontrolle des BND finden sich darin weitaus weniger Passagen als im ersten Abhörurteil zur Kontrolle des Verfassungsschutzes. Das Bundesverfassungsgericht verweist wiederholt auf seine damals etablierten Grundsätze.

(3) Drittes Abhörurteil

15 Jahre nach der zweiten Abhörentscheidung entschied das Bundesverfassungsgericht erneut über die Verfassungsmäßigkeit der strategischen Fernmeldeüberwachung durch den BND.¹⁹² Verfahrensgegenstand waren die Befugnisse zur Überwachung der Objekte, Aufzeichnung und Auswertung der damit verbundenen Daten sowie deren Übermittlung an andere Behörden gemäß dem im Jahre 1994 novellierten G 10. Die angegriffene Gesetzesänderung erweiterte die Reichweite der strategischen Überwachung durch den BND erheblich.

Die Richter beschreiben einleitend den Gewährleistungsgehalt von Art. 10 GG und stellen fest, dass sich die im Volkszählungsurteil¹⁹³ zu Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG entwickelten Vorgaben auf Art. 10 GG „weitgehend übertragen lassen“.¹⁹⁴ Unter

¹⁸⁸ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 74.

¹⁸⁹ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 75.

¹⁹⁰ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 76.

¹⁹¹ BVerfG, Beschluss v. 20.6.1984 - 1 BvR 1494/78.

¹⁹² BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95.

¹⁹³ BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83.

¹⁹⁴ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 164 ff., dazu gehören u.a. der Zweckbindungsgrundsatz und der grundsätzliche Anspruch auf Kenntnis von der Datenverarbeitung, vgl. *Müller-Terpitz*, Jura 2000, 296, 299.

anderem ergebe sich aus Art. 10 GG ein datenschutzrechtlicher Anspruch des Betroffenen auf Kenntnis der Fernmeldeüberwachung. Dieser könne begrenzt werden, wenn die Maßnahme durch die Kenntnisaufnahme ihren Zweck verfehlen würde, insoweit gelte der Gesetzesvorbehalt des Art. 10 Abs. 2 GG. Diese Mitteilungsbeschränkung in Kombination mit der Heimlichkeit der Fernmeldeüberwachung verursache Rechtsschutzlücken, die Art. 10 GG insofern adressiere, dass aus ihm die Notwendigkeit einer unabhängigen, weisungsfreien Kontrolle durch staatliche Organe und Hilfsorgane folge. Diese bereits im ersten Abhörurteil etablierten Grundsätze konkretisiert der Erste Senat vorsichtig: Zwar habe der Gesetzgeber bei der Ausgestaltung einen Beurteilungsspielraum, die Kontrolle sei jedoch nur „wirksam“, wenn sie sich „auf alle Schritte des Prozesses der Fernmeldeüberwachung“ erstrecke, das heißt sowohl die Datenerfassung als auch -verwertung umfasse.¹⁹⁵

Neben der Rechtmäßigkeit müsse kontrolliert werden, ob die gesetzlichen Schutzvorkehrungen eingehalten würden.¹⁹⁶ Die Richter weisen darauf hin, dass eine Protokollierung von Datenverarbeitungen die notwendige Voraussetzung einer „hinreichenden Kontrolle“ sei.¹⁹⁷

Außerdem formulierten sie zwei weitere Kontrollvorgaben: Erstens müsse wegen der „erheblich ausgeweiteten Überwachungstätigkeit“ sichergestellt sein, dass die G 10 – Kommission „personell so ausgestattet ist“, dass sie ihrer Aufgabe „in effektiver Weise“ nachkommen kann. Zweitens müsse in der Landesverwaltung eine „ausreichende Kontrolle“ existieren, soweit Daten aus Fernmeldeüberwachungen dorthin übermittelt würden.¹⁹⁸

dd) Frühere Sonderstellung von Art. 10 GG

Die Bedeutung von Art. 10 GG war lange Zeit hervorgehoben, denn bei anderen, ebenfalls eingriffsintensiven, aber nicht Art. 10 GG, sondern andere Grundrechte betreffende Maßnahmen wie beispielsweise dem Einsatz von Verdeckten Mitarbeitern, war der Rechtsweg wegen der Heimlichkeit de facto ausgeschlossen und eine kompensierende Kontrolle nicht vorgesehen. Spätestens mit der enormen technischen Weiterentwicklung und der damit verbundenen Erweiterung nachrichtendienstlicher Mittel um Befugnisse wie beispielsweise die Online-Durchsuchung war es nicht mehr überzeugend, dass nur die Eingriffe gem. Art. 10 Abs. 2 S. 2 GG einer alternativen Kontrolle unterliegen sollen.

¹⁹⁵ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 169-171, 302.

¹⁹⁶ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 169-171.

¹⁹⁷ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 280, hier bezogen auf Datenübermittlungen.

¹⁹⁸ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 304.

Mit der Herleitung von Transparenzvorgaben und Kontrollanforderungen aus der Verhältnismäßigkeitsprüfung¹⁹⁹ hat sich die „Sonderstellung“ von Art. 10 Abs. 2 S. 2 GG aufgelöst. Mittlerweile leitet das Bundesverfassungsgericht die Transparenz- und Kontrollvorgaben selbst in den Entscheidungen, bei denen der grundrechtliche Maßstab eigentlich Art. 10 GG ist, aus der Verhältnismäßigkeitsprüfung und nicht aus Art. 10 Abs. 2 S. 2 GG ab.²⁰⁰

ee) Kein ausschließliches Kontrollmandat der G 10-Kommission

Bisher hat das Bundesverfassungsgericht sich nicht explizit dazu geäußert, wie die richterähnliche Vorabkontrolle und die Datenschutzkontrolle im Anwendungsbereich von Art. 10 Abs. 2 S. 2 GG voneinander abgegrenzt werden sollen. Ein Abgrenzungsproblem besteht nur bei Maßnahmen, die in Art. 10 GG eingreifen, weil Art. 10 GG das Recht auf informationelle Selbstbestimmung (RaiS), aus dem grundsätzlich die Notwendigkeit der Datenschutzkontrolle hergeleitet wird, in seinem Anwendungsbereich verdrängt²⁰¹. Daher stellt sich die Frage, ob Datenschutzkontrollen durch Datenschutzbeauftragte im Anwendungsbereich von Art. 10 GG ausgeschlossen werden.

In seinen aktuelleren Entscheidungen zur strategischen Überwachung hat das Bundesverfassungsgericht aus Art. 10 GG abgeleitet, dass Datenschutzkontrollen erforderlich sein können.²⁰² Deshalb wirkt sich die Schutzbereichsverdrängung des RaiS durch Art. 10 GG auf die Datenschutzkontrolle im Anwendungsbereich von Art. 10 GG im Ergebnis nicht (mehr) aus. Es ist daher davon auszugehen, dass nach Ansicht der Verfassungsrechtsprechung im Anwendungsbereich des Fernmeldegeheimnisses beide Kontrollmechanismen parallel anwendbar sind. Diese Schlussfolgerung wird durch eine Passage aus dem Urteil zum Bayrischen Verfassungsschutzgesetz gestützt: Dort be-

¹⁹⁹ Vgl. [Teil 2 A. III. 3. d.](#)

²⁰⁰ In BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 271 schreibt das Gericht: „Sieht das Gesetz Benachrichtigungspflichten nicht vor, kann Art. 10 Abs. 2 Satz 2 GG zu beachten sein. Dieser führt indes nicht zu engen verfassungsrechtlichen Vorgaben für die organisationsrechtliche Ausgestaltung einer stattdessen zu schaffenden objektivrechtlichen Kontrolle.“ Daran, dass bei Maßnahmen im Anwendungsbereich von Art. 10 Abs. 2 S. 2 GG eine richterähnliche Vorabkontrolle immer notwendig ist, ändert sich dadurch praktisch nichts, weil Maßnahmen im Anwendungsbereich von Art. 10 GG als besonders eingriffsintensiv eingeordnet werden, vgl. dazu [Teil 2 A. III. 4. b.](#) Eine Verletzung von Art. 10 Abs. 2 S. 2 GG droht bei Anwendung dieses Maßstabs daher vermutlich nicht, zumal Art. 10 Abs. 2 S. 2 GG weiterhin gültig und somit zu beachten ist.

²⁰¹ Vgl. [Teil 2 A. II.](#)

²⁰² BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 164 ff.: Das Bundesverfassungsgericht beschreibt den Gewährleistungsgehalt von Art. 10 GG und stellt fest, dass sich die in BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83 zu Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelten Vorgaben auf Art. 10 GG „weitgehend übertragen lassen“; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276.

tont das Bundesverfassungsgericht, dass es für eine effektive Datenschutzkontrolle notwendig sei, dass die kontrollierende Stelle jedenfalls „alle Überwachungsmaßnahmen, denen eine Person durch eine Behörde ausgesetzt ist, in den Blick nehmen kann“²⁰³. Die Datenschutzaufsicht kann nur dann alle Maßnahmen einer Behörde kontrollieren, wenn diejenigen Maßnahmen, die in Art. 10 GG eingreifen, ebenfalls erfasst sind.

Das geltende Recht steht hierzu teilweise in einem Spannungsverhältnis: Gemäß § 28 Abs. 2 S. 2 BVerfSchG (i. V. m. § 63 BNDG bzw. § 13a MADG) ist der Bundesbeauftragte für den Datenschutz nicht zuständig, soweit „die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt“ und die G 10-Kommission den BfDI nicht um Kontrollen ersucht hat. Das ist grundsätzlich unproblematisch, da die Datenschutzkontrolle nicht dem BfDI obliegen muss²⁰⁴, sondern auch der G 10-Kommission übertragen sein kann. Allerdings ist das Kontrollmandat der G 10-Kommission auf die Vorschriften nach dem G 10 begrenzt, § 15 Abs. 5 G 10. Um Kontrolllücken zu vermeiden, wird die Norm so verstanden, dass der BfDI für die Kontrollen der übrigen Normen zuständig ist, soweit das G 10 keine spezielleren Vorgaben errichtet.²⁰⁵ Das bedeutet, dass der BfDI Zugang zu aus G 10-Maßnahmen erlangten Informationen haben muss.²⁰⁶ Demnach darf der BfDI nach geltendem Recht beispielsweise Dateisysteme auf ihre Datenschutzkonformität hin überprüfen, obwohl G 10-Daten darin enthalten sind.²⁰⁷ § 28 Abs. 2 S. 2 BVerfSchG steht einem potenziellen Gesamtüberblick des BfDI demnach nicht entgegen. Die G 10-Kommission hingegen, die de lege lata für die Datenschutzkontrolle nach dem G 10 zuständig ist, kann wegen ihrer eng umgrenzten Zuständigkeit gem. § 15 Abs. 5 G 10, § 8b BVerfSchG nicht alle Maßnahmen in den Blick nehmen, denen eine Person durch eine Behörde ausgesetzt ist. Da die G 10-Kommission insoweit als Datenschutzkontrolleur agiert, müsste ihr nach der neuesten Rechtsprechung Kenntnis aller Überwachungsmaßnahmen gewährt werden.

²⁰³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 Rn. 290.

²⁰⁴ Vgl. [Teil 2 A. III. 1. a. cc](#); Schenke/Graulich/Ruthig/Siems, § 26 a BVerfSchG Rn. 6.

²⁰⁵ Schenke/Graulich/Ruthig/Siems, § 26a BVerfSchG Rn. 7; Löffelmann/Zöller, Nachrichtendienstrecht, S. 249.

²⁰⁶ BT-Drs. 18/11325, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 v. 24.2.2017, S. 122: „Die Zuständigkeitsabgrenzung soll lediglich Doppelzuständigkeiten – mit dem Risiko konträrer Ergebnisse – ausschließen, anders als der bisherige § 24 Absatz 2 Satz 3 BDSG a. F. jedoch nicht vor Kenntnisnahme durch den oder die Bundesbeauftragte schützen, soweit solche Kenntnis für seine bzw. ihre – anderen – Kontrollaufgaben erforderlich ist.“

²⁰⁷ BT-Drs. 18/11325, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 v. 24.2.2017, S. 122; Schenke/Graulich/Ruthig/Siems, § 26a BVerfSchG Rn. 7.

Ob vergleichbare Normen in den Landesverfassungsschutzgesetzen²⁰⁸ ähnlich ausgelegt werden und somit im Einklang mit der neuesten Rechtsprechung einem Kontrolleur einen potenziellen Gesamtüberblick verschaffen, ist unklar.

b. Art. 13 GG

Technische Mittel zur Überwachung von Wohnraum dürfen gem. Art. 13 Abs. 3 und 4 GG nur eingesetzt werden, wenn eine richterliche Anordnung vorliegt. Bei Wohnraumüberwachungen zu repressiven Zwecken sind nur akustische Überwachungen möglich, für ihre Anordnung ist ein Spruchkörper mit drei Richtern, im Eilfall ein Einzelrichter zuständig (Art. 13 Abs. 3 GG). Im Übrigen ist die Ausgestaltung des Richtervorbehalts dem Gesetzgeber überlassen, soweit die Kontrolle hinreichend wirksam ausgestaltet ist.²⁰⁹

In der Gefahrenabwehrkonstellation darf zusätzlich mit optischen Mitteln überwacht werden. Die nähere Ausgestaltung der richterlichen Vorabkontrolle ist dem einfachen Gesetzgeber überlassen. Bei Gefahr im Verzug kann eine behördliche Stelle entscheiden, die richterliche Entscheidung muss jedoch unverzüglich nachgeholt werden (Art. 13 Abs. 4 GG).

c. Art. 1 Abs. 1 GG

Das Kernbereichsschutzkonzept hat das Bundesverfassungsgericht aus einzelnen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG entwickelt.²¹⁰ Bei den sogenannten „verletzungsgeneigten“ Befugnissen müssen stets Kernbereichsschutzvorkehrungen getroffen werden.²¹¹ Auf die Eingriffsintensität kommt es anders als bei den richterähnlichen Vorabkontrollen und den Datenschutzkontrollen nicht an. Dass die Kernbereichsrelevanz die Eingriffsintensität steigert, ändert nichts daran, dass für die zwingende Anwendung des Schutzkonzepts bereits ihr Vorliegen ausschlaggebend ist.

²⁰⁸ § 6 Abs. 1 [AG G 10 RP](#); § 30 Abs. 1 S. 2 [LVerfSchG RP](#); § 17 Abs. 1 S. 2 [BWLVS](#); § 15 Abs. 2 S. 3 [VSG NRW](#); § 23 b Abs. 2 S. 2 [HmbVerfSchG](#); § 27 Abs. 3 [SächsVSG](#); Umkehrschluss aus § 5 Abs. 3 S. 1 [AG G 10 LSA](#); § 3 Abs. 1 [AG G 10 MV](#); § 32 a Abs. 2 S. 2 [VSG Bln](#); *Aden*, Vorgänge 2015, 245, 248.

²⁰⁹ BVerfG, Urteil v. 3.3.2004 - 1 BvR 2378/98 - Rn. 270 ff.

²¹⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 275.

²¹¹ Vgl. [Teil 2 A. III. 2. b.](#)

d. Verhältnismäßigkeitsgrundsatz

Darüber hinaus entwickelte das Bundesverfassungsgericht Anforderungen an die Kontrolle aus der Verhältnismäßigkeitsprüfung. Bezeichnet wird die Ableitung von Kontrollvorgaben aus der Verhältnismäßigkeit als Grundrechtsschutz „durch Verfahren“.²¹²

Die Herleitung der Vorabkontrolle (aa)) unterscheidet sich von der der Datenschutzkontrollen (bb)) und Kernbereichsschutzvorgaben (cc)).

aa) Vorabkontrolle

Das Bundesverfassungsgericht verknüpft die verfassungsrechtlichen Anforderungen an die Kontrolle mit dem Eingriffsgewicht: Je tiefer das Eingriffsgewicht, desto intensiver müsse der Eingriff durch Kontrolle begleitet sein. Bei intensiven Grundrechtseingriffen sei eine unabhängige richterliche oder richterähnliche Vorabkontrolle unabdingbar.²¹³ Das gilt unabhängig davon, in welches Grundrecht eingegriffen wird.

bb) Datenschutzkontrollen

Das Volkszählungsurteil²¹⁴ ist für die verfassungsrechtliche Herleitung der Datenschutzkontrolle von herausragender Bedeutung, weil das Bundesverfassungsgericht darin festgelegt hat, dass an staatlichen „Datenverwendungen“ wegen des damit verbundenen Eingriffs in das RaiS grundsätzlich unabhängige Datenschutzkontrollen beteiligt sein müssen.²¹⁵ In seiner Rechtsprechung hat das Gericht für heimliche Maßnahmen der Sicherheitsbehörden hiervon keine Ausnahme gemacht, sodass unabhängige

²¹² U.a. in BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 257, „verfahrensrechtlich[e]“ Absicherung der Betroffenenrechte; *Kutscha*, NVwZ 2003, 1296, 1300; *Thomé*, Reform der Datenschutzaufsicht, S. 94 betitelt die Pflicht zur Datenschutzkontrolle als Schutzpflicht, die Datenschutzkontrolle bewirke eine „organisatorische und verfahrensmäßige Absicherung des materiellen Grundrechtsschutzes“; kritisch *Alt*, Kompensatorische Kontrolle, S. 242, 291 f.

²¹³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214 ff.; BVerfG - Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 257, 259; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 248; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09. Das BVerfG schreibt in BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259 zwar bei „Grundrechtseingriffen von besonders schwerem Gewicht“ sei nur ein Richtervorbehalt noch verhältnismäßig, in der nächsten Randnummer konkretisiert es dann jedoch, dass eine „andere Stelle“ mit der Kontrolle betraut werden dürfe, wenn sie genauso unabhängig und neutral sei wie ein Richter; *Bantlin/Graulich*, GSZ 2023, 179, 181; *Alt*, Kompensatorische Kontrolle, S. 239.

²¹⁴ BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83.

²¹⁵ BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83 - Rn. 155; dies gilt generell für jede Datenverarbeitung, unabhängig von ihrer Erhebungsweise oder bestimmter Datenkategorien, vgl. *Denninger*, KJ 1985, 215, 228.

Datenschutzkontrollen notwendig sind. Detailliertere Anforderungen an die Datenschutzkontrolle im Sicherheitsrecht leitet das Bundesverfassungsgericht – wie bei den richterähnlichen Vorabkontrollen – aus der Verhältnismäßigkeit ab.²¹⁶ Dabei werden die Anforderungen im Urteil zur Antiterrordatei²¹⁷ und zum Bundeskriminalamts-gesetz²¹⁸ im Unterschied zur richterlichen bzw. richterähnlichen Vorabkontrolle nicht vergleichbar ausdrücklich an die Eingriffsintensität geknüpft, sondern genereller etabliert.

Anders verhält es sich in der Entscheidung zur strategischen Auslands-Fernmelde-aufklärung²¹⁹: Das Gericht folgert aus der hohen Eingriffsintensität präzisere verfassungsrechtliche Anforderungen an die Ausgestaltung der Datenschutzkontrolle.²²⁰ Bemerkenswert ist, dass der grundrechtliche Maßstab dieser Entscheidung Art. 10 GG (und Art. 5 Abs. 1 S. 1 Hs. 1 GG) ist. Das bedeutet, dass das Bundesverfassungsgericht die Maßgaben der Datenschutzkontrolle nicht ausschließlich aus dem RaiS, sondern auch aus Art. 10 GG ableitet. Bereits in seiner vorherigen Entscheidung zu Art. 10 GG, schrieb das Bundesverfassungsgericht:

„Vielmehr ergeben sich aus Art. 10 GG auch besondere Anforderungen an den Gesetzgeber, die gerade die Verarbeitung personenbezogener Daten betreffen, welche mittels Eingriffen in das Fernmeldegeheimnis erlangt worden sind. Insoweit lassen sich die Maßgaben, die das Bundesverfassungsgericht im Volkszählungsurteil aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat (vgl. BVerfGE 65, 1 <44 ff.>), weitgehend auf die speziellere Garantie in Art. 10 GG übertragen“²²¹

²¹⁶ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 214 f.; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 141; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 276; so auch *Alt*, Kompensatorische Kontrolle, S. 239.

²¹⁷ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07.

²¹⁸ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09.

²¹⁹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17.

²²⁰ *Alt* führt demgegenüber die detaillierten Anforderungen aus der Entscheidung zur strategischen Auslands-Fernmeldeüberwachung nicht nur auf die hohe Eingriffsintensität zurück, sondern geht davon aus, dass die in BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 entworfenen „völlig neu(en)“ administrativen und gerichtsähnlichen Kontrollstrukturen verfassungsrechtlich dann erforderlich sind, wenn die „Funktionsfähigkeit der herkömmlichen Rechtskontrolle (...) stark zurückgenommen“ ist, etwa, weil Betroffene nicht benachrichtigt werden, *Alt*, Kompensatorische Kontrolle, S. 240.

²²¹ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 164.

Dafür, dass die Datenschutzkontrolle eine solche zu *übertragende Maßgabe* aus dem Volkszählungsurteil ist, spricht, dass das Bundesverfassungsgericht im Zusammenhang mit der Kontrolle durch unabhängige Organe und Hilfsorgane als Referenz auf das Volkszählungsurteil verweist²²².

Somit bleibt festzuhalten, dass die Datenschutzkontrolle auf Basis des RaiS seit dem Volkszählungsurteil für alle Datenverarbeitungen vorgeschrieben war und aufgrund der höchstrichterlich entschiedenen Übertragbarkeit dieser Rechtsprechung auf Art. 10 GG mittlerweile auch in dessen Anwendungsbereich etabliert ist. Die Details der Ausgestaltung ergeben sich wiederum aus Verhältnismäßigkeitserwägungen und sind als Konsequenz der neuesten Rechtsprechung an die Eingriffsintensität geknüpft.

cc) Eingriffsintensität als entscheidender Faktor

Seit dem Grundsatzurteil zum Bundeskriminalamtsgesetz 2016 werden die Kontrollanforderungen, die aus der Verhältnismäßigkeit hergeleitet werden, von der Eingriffsintensität der jeweiligen Maßnahme abhängig gemacht.²²³ Während dem Gesetzgeber grundsätzlich ein Gestaltungsspielraum verbleibt, zieht das Bundesverfassungsgericht bei der Kontrolle von schweren Eingriffen eine verfassungsrechtliche Grenze. Dann ist eine richterliche oder richterähnliche Vorabkontrolle des Eingriffs zwingend geboten.²²⁴

Im Gegensatz dazu ist die Datenschutzkontrolle unabhängig von der Eingriffsintensität zunächst für alle staatlichen Datenverarbeitungen notwendig. Allerdings richten sich die Detailanforderungen an Kontrolle auch nach der Eingriffsschwere. Aufgrund ihrer Eingriffsintensität besteht bei der strategischen Überwachung fast kein Regelungsspielraum mehr. Das heißt, dass die Datenschutzkontrolle zwar nicht mit der Eingriffsintensität begründet wird, hinsichtlich der Ausgestaltung jedoch von ihr abhängig ist.

4. Eingriffsintensität nachrichtendienstlicher Mittel

Da die Eingriffsintensität einer Maßnahme darüber entscheidet, welches Kontrolldesign verfassungsrechtlich zwingend ist²²⁵, muss die Eingriffsintensität der Befugnisse beurteilt werden.

²²² BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 171.

²²³ BVerfG, Urteil v. 20.4.2016, 1 BvR 966/09 - 1 BvR 1140/09 - Rn.117.

²²⁴ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 257, 259; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 Rn. 248; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn.117; BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 203, 252; BVerfG, Beschluss v. 10.11.2020 - 1 BvR 3214/15 - Rn. 89; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 152, 214.

²²⁵ Alt, Kompensatorische Kontrolle, S. 240.

a. Faktoren zur Festlegung der Eingriffsintensität im Sicherheitsrecht

Welche Eingriffsintensität einer staatlichen Maßnahme beizumessen ist, entscheidet das Bundesverfassungsgericht im Einzelfall anhand einer „wertende[n] Gesamtbetrachtung“, bei der es unterschiedliche Kriterien so miteinander ins Verhältnis setzt, dass sie einander in ihrer Wirkung entweder kompensieren oder die Intensität des Eingriffs verstärken.²²⁶ Die Kriterien lassen sich in verschiedene Kategorien einsortieren, unter anderem nach „Art, Umfang und denkbare[r] Verwendung der Daten“ sowie der Gefahr ihres Missbrauchs.²²⁷

Tanneberger unterscheidet auf Basis dieser verfassungsgerichtlichen Einordnung „fünf übergeordnete Gesichtspunkte“: Erstens die Art der Information, zweitens den Anlass für die Erhebung, drittens die Umstände der Erhebung, viertens den betroffenen Personenkreis und fünftens die denkbare Verwertung der Daten. Er stellt fest, dass keiner dieser Gruppen ein erhöhtes Gewicht beigemessen wird, sondern dass es auf den zu beurteilenden Einzelfall ankommt. Außerdem weist er darauf hin, dass sich manche Kriterien in mehr als eine der Kategorien einsortieren lassen. Wo das Vorliegen eines Kriteriums eingriffserschwerend wirkt, kann sein Nichtvorliegen eingriffsmildernd eingestellt werden; grundsätzlich sucht das Bundesverfassungsgericht ausgehend von einem einfachen Grundrechtseingriff aber nach intensivierenden Kriterien.²²⁸

An seinen Überlegungen ist die folgende Darstellung und Aufzählung der Kriterien orientiert, ergänzt um die Kriterien aus der neueren Rechtsprechung und um spezifisch nachrichtendienstliche Aspekte. Die Aufzählung ist nicht abschließend, sondern beinhaltet die häufigsten Kriterien.

aa) Art der Daten

Wenn gezielt personenbezogene Daten erhoben werden, erhöht das die Eingriffstiefe. Entsprechend sinkt sie grundsätzlich bei einer strategischen Überwachung (*Personenbezug*).²²⁹ Dass bei einer strategischen Überwachung im Vergleich zu der in der Vergan-

²²⁶ *Tanneberger*, Sicherheitsverfassung, S. 233.

²²⁷ BVerfG 1 BvR 1547/19 - 1 BvR 2634/20 v. 16.2.2023 - Rn. 76, auf Art, Umfang und Verwendungsmöglichkeit abstellend BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 206.

²²⁸ *Tanneberger*, Sicherheitsverfassung, S. 236 ff., 254 f.

²²⁹ BVerfG, Beschluss vom 20.6.1984 - 1 BvR 1494/78 - Rn. 59; BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 233; BVerfG, Beschluss v. 10.11.2020 - 1 BvR 3214/15 - Rn. 96; *Tanneberger*, Sicherheitsverfassung, S. 239.

genheit eingesetzten Technik heute gezielt personenbezogene Überwachungen möglich sind, hat das Bundesverfassungsgericht beispielsweise eingriffsintensivierend gewertet.²³⁰

Darüber hinaus hängt die Eingriffsintensität davon ab, welche Daten erhoben werden. Ist eine Maßnahme potenziell geeignet, Informationen aus dem Kernbereich der privaten Lebensgestaltung²³¹ zu erheben, verstärkt dies den Eingriff.²³² Selbst wenn die Schwelle zur kernbereichsrelevanten Information nicht überschritten ist, die Daten sich aber auf persönliche Kommunikationsbeziehungen mit „privatem Charakter“ erstrecken können, wirkt dies eingriffsintensivierend (*Kernbereichsrelevanz u. sonstige Betroffenheit des Privatlebens*).²³³

Als besonders sensibel einzustufende Daten, wie beispielsweise Informationen über den Kontoinhalt und Kontobewegungen, erhöhen das Eingriffsgewicht (*Sensibilität*).²³⁴ Eingriffsmindernd muss hingegen berücksichtigt werden, wenn die Daten nichts über die Umstände oder den Inhalt von Kommunikation aussagen, sondern sich rein auf den zugrundeliegenden Vertrag beziehen (Bestandsdaten).²³⁵

Erfolgt ein Zugriff auf Daten, die aus einem *geschützten Vertrauensverhältnis* wie zum Beispiel aus einer Beziehung zwischen Rechtsanwalt und Mandant stammen, verstärkt dies den Eingriff.²³⁶

Entscheidend ist darüber hinaus der Umfang der erhobenen Daten über eine Person (*subjektive Datenkumulation*).²³⁷ Moderne Geräte, wie Computer und Smartphones, beinhalten oft sensible Daten über das Privatleben, über Kommunikationspartner und Gepflogenheiten einer Person.²³⁸ Greift der Staat beispielsweise im Rahmen einer Online-Durchsuchung auf diese Daten zu, erhält er einen umfangreichen Datensatz und somit einen tiefen Einblick in die Persönlichkeit, was den Eingriff intensiviert. Auch längerfristige Maßnahmen bewirken eine Datenkumulation.²³⁹

²³⁰ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 233; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 152.

²³¹ Def. des Kernbereichs privater Lebensgestaltung vgl. [Teil 2 A. II](#). Als Beispiel kernbereichsrelevanter Informationen führt *Löffelmann* das Verhalten in der eigenen Wohnung oder Kommunikation mit nahestehenden Personen oder Personen, zu denen ein Vertrauensverhältnis besteht, an, *Löffelmann*, GSZ 2019, 190, 191.

²³² BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 217 m. w. N.

²³³ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 104; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 147; BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 253; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 217.

²³⁴ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 297, 322; *Tanneberger*, Sicherheitsverfassung, S. 240.

²³⁵ BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 140, 168.

²³⁶ *Löffelmann*, Hdb. des Rechts der Nachrichtendienste, 1093, 1103 Rn. 5.

²³⁷ *Tanneberger*, Sicherheitsverfassung, S. 241.

²³⁸ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 231.

²³⁹ *Tanneberger*, Sicherheitsverfassung, S. 241 f.

Der Umfang, die zunehmenden technischen Erhebungsmöglichkeiten und die Vielfältigkeit mancher Datenbestände erhöhen zugleich das Risiko, dass das Verhalten und die Kommunikation einer Person – über einzelne Maßnahmen hinaus – weitgehend analysiert werden können, woraus ein umfassendes Persönlichkeits- und Bewegungsprofil erstellt werden kann (*Gefahr der Erstellung eines Persönlichkeitsprofils*²⁴⁰).²⁴¹ Außerdem ist die Gefahr der Erstellung von umfassenden Persönlichkeitsprofilen mit technischen Fortschritten wie beispielsweise der intelligenten Verknüpfbarkeit von Datenbeständen gestiegen, was die Eingriffsintensität erhöht.²⁴²

Für die Verhältnismäßigkeit und die Eingriffsschwere ist weiterhin entscheidend, wie viele weitere Maßnahmen die Behörde gegenüber einer Person durchführt („*additiver Grundrechtseingriff*“).²⁴³ Soweit gegenüber der Person mehrere Befugnisse eingesetzt werden, besteht ebenfalls die Gefahr, dass die Persönlichkeit umfassend analysiert wird, was den Eingriff intensiviert.

bb) Anlass für die Informationserhebung

Für die Gewichtung der Eingriffsintensität einer Maßnahme ist zudem ihre *Streubreite* ausschlaggebend. Die Streubreite bemisst sich danach, ob und wie viele unbeteiligte Dritte, die nicht Zielpersonen sind, (zufällig) von einem Eingriff betroffen sind.²⁴⁴ Ein nachrichtendienstliches Mittel hat dann eine eingriffsintensivierende, hohe Streubreite, wenn es sich auf mehrere Unbeteiligte auswirkt und nicht einzelfallbezogen ist.²⁴⁵ Die Streubreite erhöht die Eingriffsintensität vor allem deshalb, weil sie „das Risiko systematisch steigert“, dass aufgrund „falsch positiver Wahrscheinlichkeitsurteile“ in die Grundrechte eines Betroffenen eingegriffen wird.²⁴⁶ Die strategische Überwachung hat ihrem Zweck nach beispielsweise eine sehr hohe Streubreite, weil sie Milliarden von Datenströmen analysieren soll, um potenzielle Bedrohungen erkennen zu können²⁴⁷.

²⁴⁰ Kritisch zu diesem Kriterium *Tanneberger*, Sicherheitsverfassung, S. 243, der es definiert als „Extremfälle“, [...] in denen aus bestimmten Datensätzen Einsichten über Verhaltensweisen, Vorlieben etc., kurz: persönlichkeitskonstituierende Umstände gewonnen werden können, die ihrem Gehalt nach einen Schluss auf die Persönlichkeit als Ganze zulassen“.

²⁴¹ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07 - Rn. 230, 232, 237; BVerfG, Urteil v. 2.3.2010, 1 BvR 256/08 Rn. 211 f.; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 99; BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 140, 156 ff.

²⁴² BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 Rn. 99.

²⁴³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 287 f.

²⁴⁴ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 233; *Löffelmann*, Hdb. des Rechts der Nachrichtendienste, 1093, 1103 Rn. 5.

²⁴⁵ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 233; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 101; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 210, 212.

²⁴⁶ *Bäcker*, Kriminalpräventionsrecht, S. 273 f.

²⁴⁷ U.a. BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 6, 150.

cc) *Umstände der Erhebung*

Wenn der Staat Befugnisse heimlich einsetzt, erhöht dies ihre Eingriffsintensität (*Heimlichkeit*).²⁴⁸ Dieser Aspekt ist für alle Aufklärungstätigkeiten der Nachrichtendienste relevant²⁴⁹, weil sie immer ohne Kenntnis des jeweils Betroffenen erfolgen. Das Bundesverfassungsgericht wertet es als eingriffsintensivierend, wenn dem Betroffenen infolge der Heimlichkeit der Maßnahme Einflussnahmen auf die handelnde Behörde und ein vorheriger Rechtsschutz verwehrt sind und ein nachträglicher Rechtsschutz unmöglich bzw. wesentlich erschwert ist (*ingeschränkter Rechtsschutz*).²⁵⁰

Ebenso hat die *Dauer* einer Maßnahme Auswirkungen auf ihre Eingriffsintensität. Wenn Überwachungen „längerfristig“ sind, steigert dies die Eingriffsschwere.²⁵¹ Hinsichtlich der Befugnis zur Observation (durch das BKA) müsse beispielsweise unterschieden werden, ob vereinzelt Fotos des Betroffenen erstellt werden oder ob dauerhaft Gespräche und Bilder aufgezeichnet würden.²⁵² Wird ein IMSI-Catcher dauerhaft eingesetzt, wirkt dies eingriffsintensivierend, weil der Nachrichtendienst dann ein Bewegungsprofil der Person erstellen könnte.²⁵³

Werden durch die Maßnahme Rechtsgüter von Betroffenen oder Dritten verletzt, intensiviert dies den Eingriff. Das Bundesverfassungsgericht hat beim Zugriff auf informationstechnische Systeme beispielsweise berücksichtigt, dass dieser Schäden auf dem Rechner verursachen kann (*Auswirkungen einer Maßnahme*).²⁵⁴

Wenn bei Vertragspartnern des Betroffenen Daten erhoben werden, wirkt das eingriffsintensivierend, weil dem Betroffenen dadurch in diese Vertragsverhältnis Nachteile drohen („*Publizität des Informationseingriffes*“²⁵⁵).²⁵⁶

Soweit durch die Datenerhebung *schutzwürdiges Vertrauen* des Betroffenen enttäuscht wird, steigert dies die Eingriffsintensität.²⁵⁷

²⁴⁸ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 238, 297; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 92; BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - u.a. Rn. 139, 253; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 147; *Schwabenbauer*, Hdb. des Polizeirechts, 842, 879 ff.

²⁴⁹ So auch BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 233.

²⁵⁰ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 238; „Die Rechtsschutzgarantie bleibt in Geltung, läuft aber faktisch leer.“, *Gusy*, VerwArch 2015, 437, 440.

²⁵¹ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07 - Rn. 234; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 220.

²⁵² BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 151.

²⁵³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 321.

²⁵⁴ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 240; mit weiteren Beispielen: *Tanneberger*, Sicherheitsverfassung, S. 248 f.

²⁵⁵ *Tanneberger*, Sicherheitsverfassung, S. 249.

²⁵⁶ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 322 (bzgl. von Auskunftersuchen bei Kreditinstituten).

²⁵⁷ *Bäcker*, Beschwerdeschrift BayVSG, S. 42.

dd) Betroffener Personenkreis

Wenn mehrere Personen von einer Maßnahme erfasst sind, wirkt dies eingriffsintensivierend (vgl. insoweit schon unter bb)).²⁵⁸ Wenn die Kommunikation des Betroffenen mit unbeteiligten Dritten erfasst wird, soll eingriffsverstärkend beachtet werden, dass Bürger ein berechtigtes Interesse daran haben, unbehelligt miteinander zu kommunizieren (*Erfassung der Kommunikation mit Dritten*).²⁵⁹ Darüber hinaus muss analysiert werden, inwieweit eine Maßnahme dazu geeignet ist, Personen aus Angst vor der Maßnahme bereits im Vorfeld einer möglichen Grundrechtsausübung von der Ausübung ihrer Grundrechte abzuschrecken.²⁶⁰ Als Beispiel nennt das Bundesverfassungsgericht, dass Bürger bestimmte Gesprächsinhalte vermeiden könnten.²⁶¹ Diese Abschreckung könne auch überindividuell wirken und damit die gesellschaftliche Kommunikation negativ beeinflussen (*Abschreckungswirkung*).²⁶²

ee) Denkbare Verwendung

Für die Beurteilung der Eingriffsintensität nachrichtendienstlicher Befugnisse ist zentral, dass die Nachrichtendienste zur Vorfeldaufklärung eingesetzt werden und sie – im Gegensatz zur Polizei – „unmittelbar“ selbst keine Zwangsbefugnisse einsetzen dürfen. Dies wertet das Bundesverfassungsgericht als eingriffsmindernd.²⁶³ Beachtet werden muss, dass dies nur für leichte bis mittelschwere Grundrechtseingriffe gilt; bei Maßnahmen wie der Wohnraumüberwachung oder der Online-Durchsuchung ist es wegen des sehr hohen Eingriffsgewichts der Maßnahme irrelevant, welche mittelbaren Folgen entstehen können.²⁶⁴

²⁵⁸ Tanneberger, Sicherheitsverfassung, S. 250.

²⁵⁹ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 233.

²⁶⁰ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 234; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 212.

²⁶¹ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 234; BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 Rn. 233; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 212.

²⁶² BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 234; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 212; kritisch Löffelmann, Überwachungsgesamtrechnung, S. 93.

²⁶³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 Rn. 157, 158. Es muss bezweifelt werden, ob es wirklich (auf der Linie der Rechtsprechung) eher formalistisch darauf ankommt, wer Zwangsbefugnisse einsetzt oder nicht vielmehr ausschlaggebend sein sollte, dass infolge der Informationssammlung tatsächlich Zwangsbefugnisse angewandt werden.

²⁶⁴ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 Rn. 168 f.; Bäcker, Hdb. des Polizeirechts, 109, 152 Rn. 249.

Darüber hinaus ist entscheidend, welche *Nachteile* dem Betroffenen in Folge der Maßnahmen drohen beziehungsweise von ihm befürchtet werden.²⁶⁵ So hat das Bundesverfassungsgericht beispielsweise als eingriffsintensivierend gewertet, dass durch die Speicherung in einer Verbunddatei stets mit an eine Datenabfrage anknüpfenden, belastenden Maßnahmen zu rechnen sei.²⁶⁶ Demgegenüber wirke eine enge Zweckbegrenzung eingriffsmindernd, weil durch geringere Verwendungsmöglichkeiten die Missbrauchsgefahr eingeschränkt würde.²⁶⁷ Das Bundesverfassungsgericht hat angenommen, dass Datenerhebungen und -speicherungen durch eine Vielzahl von privaten Telekommunikationsanbietern eine hohe Missbrauchsgefahr bergen, was den Eingriff intensiviert (*Missbrauchsmöglichkeiten*).²⁶⁸

Wenn Daten bevorratend und anlasslos für eine mögliche Auswertung zu einem späteren Zeitpunkt erhoben werden, intensiviert dies den Eingriff (*Bevorratungsmöglichkeit*).²⁶⁹

Soweit Befugnisse zur Weiterverarbeitung von Daten zu beurteilen sind, ist eingriffsmindernd zu beachten, dass die Daten dafür nicht neu erhoben werden müssen, sondern bei der Behörde bereits vorhanden sind (*Weiterverarbeitung*).²⁷⁰

b. Typisierte Bestimmung der Eingriffsintensität

Im Folgenden wird anhand der vom Bundesverfassungsgericht entwickelten Kriterien untersucht, welche Eingriffsintensität die wichtigsten nachrichtendienstlichen Maßnahmen haben.²⁷¹ Dabei handelt es sich um eine typisierte, von der gesetzlichen Ausgestaltung im Einzelfall unabhängige Betrachtung. Diese typisierte Untersuchung ist möglich, weil viele der Kriterien bei den jeweiligen Maßnahmen gesetzesübergreifend vorliegen und nur ihre Intensität im Einzelfall variiert. So wirkt es immer eingriffsvertiefend, wenn eine Maßnahme längerfristig möglich ist; wie schwer die Dauerhaftigkeit im Einzelfall wiegt, hängt zusätzlich davon ab, ob die jeweilige Norm eine Befristung vorsieht. Ordnet man die Maßnahmen typisiert nach ihrer Eingriffsintensität, ergeben

²⁶⁵ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 219; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 157.

²⁶⁶ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 128.

²⁶⁷ BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 173.

²⁶⁸ BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 212.

²⁶⁹ Zur bevorratenden Speicherungsmöglichkeit von Verkehrsdaten, BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 153.

²⁷⁰ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 111.

²⁷¹ Ähnlich *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, S. 20 ff.

sich daraus allgemeine, gesetzesübergreifende Leitlinien für die Ausgestaltung ihrer verfahrensrechtlichen Sicherungen und des notwendigen Kontrollmechanismus.²⁷²

Bei allen Befugnissen der Nachrichtendienste ist eingriffsintensivierend zu beachten, dass sie *heimlich* erfolgen. Darüber hinaus ist grundsätzlich davon auszugehen, dass die Betroffenen *identifizierbar* sind. Soweit die Nachrichtendienste aus offenen Quellen frei zugängliche Informationen erheben, liegt kein Grundrechtseingriff vor.²⁷³

Insgesamt sind vier Eingriffsstufen zu unterscheiden.²⁷⁴

aa) Besonders schwere Grundrechtseingriffe

Dazu, welche nachrichtendienstlichen Mittel die Grundrechte am intensivsten beeinträchtigen, hat das Bundesverfassungsgericht sich mehrfach geäußert.

(1) Wohnraumüberwachung und Online-Durchsuchung

Bei der Wohnraumüberwachung handelt es sich nach ständiger Rechtsprechung um einen (besonders) schweren Grundrechtseingriff, insbesondere, weil der Staat mit Hilfe solcher Maßnahmen tief in die *Privatsphäre* einer Person eindringen und höchstvertrauliche Situationen erfassen kann.²⁷⁵

Vergleichbar schwer wie die Wohnraumüberwachung wiegt die Online-Durchsuchung, weil auch hier die Gefahr besteht, dass die Persönlichkeit weitgehend ausgespäht wird.²⁷⁶ Dafür spricht, dass Betroffene in ihren informationstechnischen Systemen sehr private „tagebuchartige“ Daten (beispielsweise Ton- und Bilddateien) speichern können.²⁷⁷ Außerdem kann der Staat bei der Online-Durchsuchung auf – im Vergleich mit

²⁷² Im Übrigen benennt auch das BVerfG die Eingriffsintensität bestimmter Maßnahmen allgemein typisierend wie beispielsweise bei der Wohnraumüberwachung in BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 180.

²⁷³ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 308.

²⁷⁴ *Bäcker*, Hdb. des Verfassungsrechts, 1715, 1745 Rn. 93. Das Bundesverfassungsgericht verwendet bezüglich der Eingriffsschwere keine einheitliche Terminologie, vgl. *Tanneberger*, Sicherheitsverfassung, S. 234 ff.; *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 382 f.

²⁷⁵ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 180, 192; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 168 f., 177, demnach kommt es aufgrund der Eingriffsschwere insbesondere auch nicht darauf an, ob eine Polizeibehörde oder ein Nachrichtendienst handelt.

²⁷⁶ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 230; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 192 BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 168; *Bäcker*, Eingriffstatbestände, 137, 148; ebenso *Schwabenbauer*, Hdb. des Polizeirechts, 842, 903 f.

²⁷⁷ „Über die auf dem Rechner verfügbaren Dokumente der Betroffenen, bspw. zu deren Gedanken, finanziellen und medizinischen Daten, ist es einem Angreifer praktisch möglich, ‚den Menschen in die Köpfe zu schauen‘“, *Lachenmann*, DöV 2016, 501, 504; m. Verweis auf James Badford, *Greenwald*, Globale Überwachung, S. 285.

anderen Befugnissen – umfangreichere Datenmengen zugreifen (*subjektive Datenkumulation*). Daher birgt die Online-Durchsuchung das Risiko, dass *Verhaltensprofile* erstellt werden. Mit der Online-Durchsuchung kann Kommunikation aufgezeichnet werden, was das Interesse des Einzelnen an *unbeobachteter Kommunikation* beeinträchtigt. Indem Kommunikation mit Dritten erfasst sein kann, erhöht sich die *Streubreite*. Die Online-Durchsuchung verstärkt zudem die Furcht vor Überwachung und kann deshalb eine gesamtgesellschaftliche *Abschreckungswirkung* entfalten. Soweit die Befugnis zur *längerfristigen* Überwachung ermächtigt, steigt dadurch die Eingriffsintensität. Darüber hinaus muss bei der Online-Durchsuchung eingriffsschwerend bedacht werden, dass durch den Zugriff auf das informationstechnische System *Schäden* verursacht werden können.²⁷⁸

Sowohl die Wohnraumüberwachung als auch die Online-Durchsuchung sind nach der Überzeugung des Bundesverfassungsgerichts für sich genommen so eingriffsintensiv, dass es in der Bewertung der Eingriffsintensität nicht darauf ankommt, dass dem Verfassungsschutz unmittelbar keine Zwangsbefugnisse zur Verfügung stehen.²⁷⁹

(2) Eingriffe in informationstechnische Systeme von Ausländern im Ausland

Die Rechtsgrundlage für Eingriffe in informationstechnische Systeme von Ausländern im Ausland (§§ 34 ff. BNDG) hat den Zweck, dem BND Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen von Ausländern im Ausland zu ermöglichen. Dementsprechend sind die Ausführungen zur Online-Durchsuchung auf diese Maßnahme übertragbar. Es handelt sich um einen besonders schweren Grundrechtseingriff.²⁸⁰

Das gilt selbst dann, wenn die Maßnahme in der Praxis überwiegend dazu genutzt werden soll, staatliche informationstechnische Systeme zu überwachen²⁸¹. Dass es beim Zugriff auf staatliche Systeme nicht darum geht, Persönlichkeitsprofile zu erstellen, könnte zwar grundsätzlich eingriffsmindernd gewertet werden. Allerdings ist nach der

²⁷⁸ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 231 ff.

²⁷⁹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 169.

²⁸⁰ Dabei handle es sich um „eines der schwerwiegendsten Aufklärungs- und Ermittlungsinstrumente“, *Löffelmann/Zöller*, Nachrichtendienstrecht, S. 191 Rn. 70; „(...) bedeutenden Schwere des Grundrechtseingriffs“, *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12.

²⁸¹ BT-Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 95; Die Befugnis werde nicht individuell gegenüber bestimmten Personen angewandt, individuell sei zunächst nur „die technische Herangehensweise: Daten werden hier nicht mehr im Netz abgefangen und mit Hilfe von Suchbegriffen durchforstet, sondern heimlich aus IT-Systemen ausgelesen“, *Steiner*, GSZ 2023, 124, 129.

Rechtsprechung des Bundesverfassungsgerichts entscheidend, welche „Einsatzmöglichkeiten“ eine Befugnis „tatsächlich“ schafft.²⁸² Weil die Rechtsgrundlage nicht differenziert und damit auch Online-Durchsuchungen von ausländischen Privatpersonen ermöglicht, handelt es sich um einen besonders schweren Eingriff.

Die Maßnahme ist ausweislich der Entwurfsbegründung der Bundesregierung sogar eingriffsintensiver als die strategische Ausland-Fernmeldeaufklärung, denn sie werde im Gegensatz zu strategischen Ausland-Fernmeldeüberwachung „immer ‚individuell‘ angeordnet, d. h. bestimmt oder bestimmbar in Richtung einer oder mehrerer natürlicher oder juristischer Personen oder einer Gruppierung natürlicher oder juristischer Personen im Ausland, die durch einen zugrundeliegenden Sachverhalt miteinander verbunden sind (...) oder gegen ein informationstechnisches System im Ausland, welches eindeutig benannt und identifiziert werden kann.“²⁸³

(3) *Strategische Überwachung*

Die strategische Überwachung (sowohl nach G 10 als auch nach dem BNDG) ist ein besonders schwerer Grundrechtseingriff²⁸⁴; Sie erfolgt *anlasslos* und mit einer sehr hohen *Streubreite*²⁸⁵, zudem werden die Daten *bevorratend* für eine mögliche Auswertung zu einem späteren Zeitpunkt erhoben. Die gewonnenen Informationen können sehr *private* Kommunikation beinhalten sowie sich auf Bilder, Dateien und das Nutzungsverhalten im Internet erstrecken. Dass heutzutage im Rahmen der strategischen Überwachung technisch gezielte *personenbezogene* Überwachungen möglich sind, muss eingriffsintensivierend berücksichtigt werden.²⁸⁶ Durch Verknüpfung der auf diese Weise gewonnen Daten können *Persönlichkeitsprofile* erstellt werden.²⁸⁷ Als eingriffsmindernd wertet das Bundesverfassungsgericht, dass dem Betroffenen bei der strategischen Überwachung im Ausland (zunächst) keine Folgen drohen, weil der BND dort nicht

²⁸² BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 322 ff., 326.

²⁸³ BT-Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 95.

²⁸⁴ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 146, 151 ff.; *Bäcker*, Beschwerdeschrift G 10, S. 29 ff.; *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 393, 421 f.

²⁸⁵ Zur unterschiedlich hohen Streubreite der strategischen Überwachung gem. G 10 und der strategischen Ausland-Fernmeldeüberwachung nach BNDG, *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 396 ff., 401 ff.

²⁸⁶ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 146 ff., 151, 153; vgl. auch *Petri*, ZD 2020, 409, 411.

²⁸⁷ *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 383 ff.

über Zwangsbefugnisse verfügt, und dass die strategische Überwachung weniger zielgenau als die Beschränkung im Einzelfall sei.²⁸⁸ Dies ändert dennoch nichts daran, dass die strategische Überwachung ein besonders schwerer Eingriff ist.²⁸⁹

bb) Schwere Grundrechtseingriffe

Darüber hinaus sind die Nachrichtendienste zu einigen schweren Grundrechtseingriffen befugt.

(1) (Quellen-)Telekommunikationsüberwachung

Bei der Telekommunikationsüberwachung handelt es sich um einen schweren Grundrechtseingriff.²⁹⁰

Sie ermöglicht es, *umfangreiche* Informationen zu erheben, die sich auf die *Privatsphäre*, besondere *Vertrauensbeziehungen* und Kommunikation mit unbeteiligten Dritten (gewisse *Streubreite*) beziehen können. Es kann passieren, dass Betroffene sich im Rahmen der Telekommunikationsüberwachung zu *kernbereichsrelevanten* Themen äußern. Nicht ausgeschlossen werden kann zudem, dass *geschützte Personengruppen* abgehört werden. Die Maßnahme ermöglicht dem Nachrichtendienst, ein umfangreiches *Profil* des Betroffenen zu erstellen. Ihr Einsatz verletzt das geschützte Interesse an *unbeobachteter Kommunikation* und ist geeignet, in der Gesellschaft das Gefühl einer Bedrohung durch den Staat zu steigern (*Abschreckungswirkung*). Die Telekommunikationsüberwachung ist auch *längerfristig* möglich, was den Eingriff vertieft.²⁹¹

Die Quellen-Telekommunikationsüberwachung ist von vergleichbarem Gewicht; hinzukommt, dass durch den Einsatz der Software zur Kommunikationsausleitung möglicherweise *Schäden* an den elektronischen Geräten des Betroffenen entstehen.

(2) Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern

Vertrauensleute und Verdeckte Mitarbeiter werden gezielt eingesetzt, damit der Nachrichtendienst durch sie an Informationen gelangt, auf die er sonst keinen Zugriff hätte.

²⁸⁸ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 149.

²⁸⁹ Anderer Auffassung z.B. Gärditz, EuGRZ 2018, 6, 16.

²⁹⁰ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 223; BVerfG, Beschluss v. 12.10.2011 - 2 BvR 236/08 - Rn. 197; Schwabenbauer, Hdb. des Polizeirechts, 842, 904 Rn. 198.

²⁹¹ Gärditz ordnet die Telekommunikationsüberwachung, die mit der Verarbeitung „vorsorgend gespeicherter“ Telekommunikationsverkehrsdaten vergleichbar sei, demgegenüber einer mittleren Stufe zu, vgl. Gärditz, GSZ 2022, 161, 163.

Der Einsatz von Vertrauensleuten kann anfangs weniger intensiv sein als der von Verdeckten Mitarbeitern, weil die Vertrauensleute mit der Behörde gegebenenfalls (zunächst) wenige Informationen teilen; die Maßnahmen sind tendenziell jedoch vergleichbar einzuordnen.²⁹²

Die infolge dieser Erhebungsmethode gesammelten Daten können *umfangreich* sein und ein *Personenprofil* ermöglichen. Es ist zudem wahrscheinlich, dass auf diese Weise *privatsphären- oder sogar kernbereichsrelevante* Informationen erhoben werden. Bei ihrem Einsatz können Vertrauensleute und Verdeckte Mitarbeiter Kommunikation mit Dritten abhören (*Streubreite*). Darüber hinaus können sie Diskussionen steuern und gezielt nachfragen, was bei anderen Datenerhebungsmethoden nicht möglich ist.²⁹³ Der Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten ist geeignet, Menschen in ihrer Grundrechtsausübung *abzuschrecken* und die Angst davor kann schwerwiegende psychische Probleme verursachen.²⁹⁴ Die *Enttäuschung berechtigten Vertrauens* kann ebenfalls schwerwiegende psychische Folgen haben.²⁹⁵

Das Bundesverfassungsgericht hat betont, dass die Eingriffsintensität bei Einsätzen von Verdeckten Mitarbeitern und Vertrauensleuten von unterschiedlichen Faktoren abhängig ist: So variiert die Intensität je nach dem, *wie lange* die Personen eingesetzt werden und „welche Intensität die Beziehungen erlangen“. Hier unterscheidet das Bundesverfassungsgericht zwischen der „quantitativen“ und „qualitativen“ Intensität der Kommunikation. Die Eingriffsintensität ändere sich, je nachdem, ob die Person „lediglich einmal im Monat an einer Sitzung eines größeren Gremiums teilnimmt oder aber täglich mit einem kleinen Personenkreis in intensivem Austausch agiert“. Entscheidend sei auch, inwieweit gesamte Bestrebungen oder gezielt einzelne Personen beobachtet werden. Je tiefer die (vermeintliche) Vertrauensbeziehung werde und „je mehr private

²⁹² BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 351.

²⁹³ Roggan, GSZ 2019, 11, der davon ausgeht, dass der Einsatz von Vertrauensleuten nach der Wohnraumüberwachung und der Online-Durchsuchung die eingriffsintensivste Datenerhebungsbefugnis ist, ebenso Bergemann, Hdb. des Polizeirechts, 1225, 1266 Rn. 97; Dietrich, Hdb. des Rechts der Nachrichtendienste, 1017, 1056; gehöre zu den „schwersten denkbaren informationellen Eingriffen in Grundrechte überhaupt“, Hong, Einsatz von V-Leuten und verdeckten Mitarbeitern 2019, 45, 55 f; zur Eingriffsintensität auch Schwabenbauer: vieles spreche dafür, dass der Einsatz von V-Leuten schwerer wiege als die Telefonüberwachung, Schwabenbauer, Hdb. des Polizeirechts, 842, 904.

²⁹⁴ Bergemann, Hdb. des Polizeirechts, 1225, 1266 Rn. 97.

²⁹⁵ Bäcker, Beschwerdeschrift BayVSG, S. 43.

Informationen die Betroffenen preisgeben“, desto höher sei das Eingriffsgewicht. Besonders tief ist der Eingriff, wenn der Einsatz auf unbeteiligte Dritte abzielt, die nicht Teil der beobachteten Bestrebung sind.²⁹⁶

Je nach Einsatzmodalität ändert sich daher die Eingriffsintensität. Wenn die Verdeckten Mitarbeiter und Vertrauenspersonen nicht gezielt gegen bestimmte Personen oder nur sehr kurz eingesetzt werden und kein berechtigtes Vertrauen entsteht, ist der Eingriff mittelschwer.

Im Ergebnis ermöglichen die de lege lata sehr weit gefassten Rechtsgrundlagen zum Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten je nach Einsatzmodalität im konkreten Fall schwere Eingriffe.

(3) Längerfristige Observation

Soweit Observationen länger als 48 Stunden andauern oder an mehr als drei Tagen in einer Woche erfolgen (längerfristige Observationen), liegt wegen der *Dauer* der Maßnahme und dem *Umfang* der erfassten Äußerungen und Bewegungen ein tiefes Eindringen in die Privatsphäre und damit ein intensiver Grundrechtseingriff vor.²⁹⁷

(4) Ton- und Bildaufzeichnungen außerhalb von Wohnungen

Das Eingriffsgewicht von Ton- und Bildaufzeichnungen außerhalb von Wohnungen variiert: es kann sich um „gering[e] bis mittler[e]“ oder schwere Eingriffe handeln. Ein schwerer Eingriff liegt vor, wenn Wort und Bild des Betroffenen langfristig und *dauerhaft* aufgezeichnet werden. Wenn mehrere Maßnahmen „gebündelt“ eingesetzt werden, um „möglichst alle Äußerungen und Bewegungen zu erfassen und bildlich wie akustisch festzuhalten, können sie tief in die *Privatsphäre* eindringen und ein besonders schweres Eingriffsgewicht erlangen“. Obwohl die Überwachungen außerhalb von Wohnungen stattfinden, können „höchstvertrauliche Situationen“ erfasst werden, zum Beispiel im Auto, im Restaurant oder beim Spaziergang.²⁹⁸

In solchen „öffentlichen Rückzugsräumen“ könne eine „*berechtigte Vertraulichkeitserwartung*“ bestehen, die durch den Einsatz technischer Mittel enttäuscht

²⁹⁶ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 341 ff., 352, insbesondere macht es keinen Unterschied, dass die Vertrauensleute extern angeworben werden, da sie dem Staat zurechenbar sind (Rn. 350); vgl. auch BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 160; *Bäcker*, Eingriffstatbestände, 137, 146; zur intensitätssteigernden Wirkung eines personengerichteten Einsatzes auch *Hong*, Einsatz von V-Leuten und verdeckten Mitarbeitern 2019, 45, 56.

²⁹⁷ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 174; BVerfG, Urteil v. 26.4.2022, 1 BvR 1619/17 Rn. 357.

²⁹⁸ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 151, BVerfG, Urteil v. 26.4.2022, 1 BvR 1619/17 Rn. 357.

werde.²⁹⁹ Das Abhören des nichtöffentlich gesprochenen Wortes ist mit einem Eingriff durch eine Telekommunikationsüberwachung vergleichbar, die ebenfalls als schwerer Grundrechtseingriff gewertet wird.³⁰⁰

(5) Auskunftsverlangen gegenüber Privatunternehmen über Kontobewegungen und Verkehrsdaten

Auskunftsverlangen über Kontobewegungen und Verkehrsdaten sind schwerer zu gewichten als die übrigen Auskunftsverlangen. Das liegt daran, dass Informationen über Kontobewegungen besonders *sensibel* sind und sich anhand der Telekommunikationsverkehrsdaten ein vollständiges *Bewegungs- und Persönlichkeitsprofil* des Betroffenen erstellen lässt.³⁰¹

(6) IMSI/IMEI-Catcher

In seinem Urteil zum Bayerischen Verfassungsschutzgesetz³⁰² hat das Bundesverfassungsgericht sich erstmalig zu einer nachrichtendienstlichen Rechtsgrundlage zur Ortung von Mobilfunkgeräten geäußert und einen „schwerwiegenden Grundrechtseingriff“ angenommen.

Bei der Bestimmung der Eingriffsschwere von Rechtsgrundlagen zum Einsatz von IMSI-Catchern müsse nach der tatbestandlichen Ausgestaltung differenziert werden. Insoweit seien die rechtlichen und tatsächlichen Nutzungsmöglichkeiten der Norm entscheidend. Falls die Daten einmalig erhoben würden, läge wegen der „begrenzten Aussagekraft“ ein leichter Eingriff vor. Eine Norm, die für den Einsatz des IMSI-Catchers keine zeitliche Grenze festlege, erlaube es, den Standort wiederholt und *länger andauernd* zu ermitteln, weshalb sich ein *Bewegungsprofil* der Person erstellen lasse, was die Eingriffsintensität deutlich erhöhe.³⁰³

Unter Umständen ist (abhängig vom Wortlaut der jeweiligen Norm) das Versenden von sog. „stillen SMS“ statt dem Einsatz von IMSI/IMEI-Catchern möglich. Bei der

²⁹⁹ Bergemann, Hdb. des Polizeirechts, 1225, 1266 Rn. 96.

³⁰⁰ Löffelmann, Hdb. des Rechts der Nachrichtendienste, 1093, 1142; Bergemann weist darauf hin, dass auch der Bundesgesetzgeber zu dieser Einschätzung kommt, vgl. § 9 Abs. 3 BVerfSchG, Bergemann, Hdb. des Polizeirechts, 1225, 1266 Rn. 96.

³⁰¹ Anders beispielsweise Gärditz, der die Auskunftsverlangen gem. § 8 a BVerfSchG als von „geringerer bis mittlerer Intensität“ einordnet, Gärditz, Hdb. des Rechts der Nachrichtendienste, 967, 975.

³⁰² BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17.

³⁰³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 320 ff.: entscheidend sei, dass die Profilbildung „rechtlich oder technisch“ ausgeschlossen ist. Da es ein Ziel der Maßnahme ist, zur Vorbereitung einer TKÜ eine bestimmte Mobilfunknummer zu identifizieren und man diese nur durch wiederholte Treffer aus vielen weiteren herausfiltern kann, ist die weniger intensive Einsatzmöglichkeit praktisch irrelevant.

stillen SMS wird einer Mobilfunknummer eine SMS gesendet, auf die das Mobilfunkgerät vom Nutzer unbemerkt in Form einer Rückmeldung an die nächstgelegene Funkzelle reagiert. Mit Hilfe der stillen SMS lassen sich demnach ebenfalls Standorte lokalisieren, sodass potenziell ein *Bewegungsprofil* erstellt werden kann.³⁰⁴

cc) Mittelschwere Grundrechtseingriffe

Einige nachrichtendienstliche Befugnisse ermächtigen zu mittelschweren Eingriffen.

(1) Einsatz von Vertrauensleuten und Verdeckten Ermittlern

Beim Einsatz von Vertrauensleuten und Verdeckten Ermittlern ist die Eingriffsintensität abhängig von der Art des Einsatzes. Wenn sie nicht gezielt gegen bestimmte Personen oder nur sehr kurz eingesetzt werden und kein berechtigtes Vertrauen entsteht, ist der damit verbundene Eingriff nur mittelschwer.³⁰⁵

(2) Sonstige Auskunftsverlangen gegenüber Privatunternehmen

Infolge der staatlichen Informationserhebung bei Privatunternehmen drohen den Einzelnen Nachteile in diesem privaten Vertragsverhältnis, was eingriffsintensivierend zu gewichten ist (*Publizität*). Grundsätzlich handelt es sich bei den erhobenen Daten um *sensible* Daten. Die durch Auskunftersuchen erhaltenen Daten dienen der (Bewegungs-) *Profilbildung* einer Person, was den Eingriff intensiviert.³⁰⁶ Soweit Telekommunikationsunternehmen zur Datenspeicherung verpflichtet werden, ist eingriffsvertiefend zu berücksichtigen, dass dadurch die *Missbrauchsgefahr* der Daten ansteigt. Allerdings wiegen nicht alle Auskunftsverlangen gleich schwer. Weil Bestandsdaten keine Profilbildung zulassen, ist die Erhebung von Bestandsdaten weniger eingriffsintensiv als die Erhebung von Verkehrsdaten.³⁰⁷

Auskunftsverlangen über Telekommunikationsbestands- und -nutzungsdaten, Flugreisedaten und Informationen von Postdienstleistern sind als mittelschwerer Eingriff einzuordnen, denn durch sie lassen sich nicht im gleichen Ausmaß Persönlichkeits- und Bewegungsprofile erstellen wie bei Telekommunikationsverkehrsdaten.

³⁰⁴ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 324.

³⁰⁵ Vgl. [Teil 2 A. III. 4. b. bb\) \(2\)](#), BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 341, 350; anders als bei der Nutzung im polizeilichen Bereich sei der Einsatz jedoch in der Regel langfristig angelegt, *Bergemann*, Hdb. des Polizeirechts, 1225, 1267 Rn. 97.

³⁰⁶ Zu Verkehrsdaten beispielsweise BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 211.

³⁰⁷ *Gärditz*, Hdb. des Rechts der Nachrichtendienste, 967, 975; zum schweren Eingriffsgewicht der Verkehrsdatenspeicherung bereits BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - Rn. 211 f.

(3) *Datenerhebung aus Social Media*

Wenn der Staat bei der Datenerhebung aus Social Media Zugangssicherungen überwindet und mit Hilfe einer Legende das Vertrauen der Kommunikationspartner in die Identität ausnutzt, sind mehrere eingriffsintensivierende Kriterien anwendbar: Es können *private* Informationen von *großem Umfang* betroffen sein (*Subjektive Datenkumulation*). Gegebenenfalls eignen sich diese Daten zur *Profilerstellung*. Die Maßnahme hat eine gewisse *Streubreite*, da innerhalb geschlossener Social Media-Bereiche in der Regel Daten mit Drittbezug geteilt werden (z.B. Fotos, die eine Gruppe von Menschen zeigen). Die Maßnahme verletzt das Interesse der Bürger an *unbeobachteter Kommunikation* und könnte deshalb *gesamtgesellschaftlich abschreckend* wirken, sodass Kommunikation weniger unbefangen erfolgt.

Vereinzelte werden die Rechtsgrundlagen zum Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern für entsprechend anwendbar erklärt.³⁰⁸ Zwischen den Maßnahmen besteht eine Ähnlichkeit insofern, dass die Social Media-Informationserhebung unter einer Legende die Fortsetzung der Tätigkeit von Vertrauensleuten und Verdeckten Mitarbeitern mit anderen Mitteln (in digitaler Form) sein kann, wenn das Vertrauen über einen vergleichbar langen Zeitraum aufgebaut wurde. Dann ist der Eingriff ebenso intensiv wie beim Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern.

(4) *Kurzfristige Observationen*

Observationen sind kurzfristig, wenn sie kürzer als 48 Stunden andauern oder an weniger als drei Tagen innerhalb einer Woche erfolgen.³⁰⁹ Durch Observationen können viele Informationen über das *Privatleben* einer Person erhoben werden, die zu einem *Bewegungs- und Persönlichkeitsprofil* zusammengestellt werden können. Soweit Personen in Kontakt mit Dritten treten, weist die Maßnahme eine gewisse *Streubreite* auf. Nach Ansicht des Bundesverfassungsgerichts handelt es sich bei einer Observation zur vereinzelt Fotoaufnahme oder „zeitlich begrenzten schlichten Beobachtung“ um geringe bis mittelschwere Eingriffe.³¹⁰

³⁰⁸ Vgl. [Teil 1 A. III. 1. k.](#), Fn. 272.

³⁰⁹ Umkehrschluss aus BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 356, wo das BVerfG die Formulierung gem. Art. 19 Abs. 1 BayVSG als „langfristige“ Observation einstuft.

³¹⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 357; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 151.

dd) Leichte Grundrechtseingriffe

Wenn der Staat durch offene Erhebung gewonnene Daten sammelt, speichert und auswertet, ist das als leichter Eingriff zu bewerten. Soweit im Rahmen einer Observation beispielsweise nur einzelne Fotos erstellt werden oder zeitlich begrenzt lediglich beobachtet wird, ist die Eingriffsintensität gering.³¹¹

Wird allerdings komplexe Auswertungstechnik eingesetzt, steigt das Eingriffsge-
wicht und variiert je nach gesetzlicher Ausgestaltung. Die Intensität ist gering, wenn eine „überschaubare“ Menge an Daten lediglich abgeglichen wird und hoch, wenn „ge-
nauer[e] Bewegungs-, Verhaltens- oder Beziehungsprofil[e]“ erstellt werden können oder Unbeteiligte dem Risiko weiterer gezielter, gegen sie gerichteter Maßnahmen aus-
gesetzt werden.³¹²

Da der Gesetzgeber bei der automatisierten Datenanalyse oder -auswertung die „we-
sentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Ver-
arbeitungsmethoden selbst durch Gesetz vorgeben“ muss³¹³ und es im Nachrichten-
dienstrecht bisher keine solche Rechtsgrundlage gibt, wird die komplexe Daten-
auswertung im Folgenden nicht weiter berücksichtigt. Sollte der Gesetzgeber die Nach-
richtendienste zu automatisierten Datenauswertungen ermächtigen, wird es sich dabei
– je nach Ausgestaltung – um einen mittleren bis (besonders) schweren Grundrechts-
eingriff handeln.

ee) Fazit

Aus der typisierten Betrachtung der nachrichtendienstlichen Befugnisse ergibt sich,
dass sie weit überwiegend mindestens mittelschwere Eingriffe bewirken. Die meisten
beschriebenen Befugnisse ermächtigen sogar zu „schweren“ oder „besonders schweren“
Eingriffen. Würde man die Tatsache mit einbeziehen, dass die nachrichtendienstlichen
Befugnisse additiv eingesetzt werden, würde dies die Intensität zusätzlich steigern.

ff) Abweichende Bewertung bei Maßnahmen des MAD?

Die Aufklärungstätigkeit des MAD als „Sonderverfassungsschutzbehörde“ der Streit-
kräfte³¹⁴ erstreckt sich unter anderem auf Bestrebungen oder Tätigkeiten von Personen,
die dem Geschäftsbereich des Verteidigungsministeriums angehören oder in ihm tätig
sind (§ 1 Abs. 1 MADG). Hierin liegt ein struktureller Unterschied zwischen dem

³¹¹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 357; *Schwabenbauer*, Hdb. des Polizeirechts, 842, 904 Rn. 198.

³¹² BVerfG, Urteil v. 16.2.2023 - 1 BvR 1547/19 - 1 BvR 2634/20 - Rn. 70 ff.

³¹³ BVerfG, Urteil v. 16.2.2023 - 1 BvR 1547/19 - 1 BvR 2634/20 - Rn. 112.

³¹⁴ Vgl. *Bäcker*, Hdb. des Verfassungsrechts, 1715, 1722; *Gusy*, ApuZ 2014, 9, 13.

MAD und den anderen Nachrichtendiensten, deren Auftrag nicht auf einen Personenkreis beschränkt ist, sondern – von der Bedrohung aus denkend – grundsätzlich jede Person erfasst. Offen ist, ob dieser Unterschied Auswirkungen auf die Bewertung der Eingriffsintensität von Maßnahmen des MAD hat. Es gibt drei Optionen: Entweder wird die Schwere von Eingriffen durch den MAD analog zu vergleichbaren Maßnahmen der anderen Nachrichtendienste bestimmt (1. Option). Alternativ könnten die Eingriffe des MAD grundsätzlich intensiver (2. Option) oder leichter (3. Option) einzuordnen sein. Die zweite und dritte Option ist nur relevant, wenn man zu der Überzeugung gelangt, dass der abweichende Auftrag des MAD im Rahmen der Eingriffskriterien zu berücksichtigen wäre.

(1) Abstrakte Kenntnis der Überwachungsmöglichkeit und Verfassungstreuepflicht

Soweit der MAD Bestrebungen oder Personen beobachtet, die dem Geschäftsbereich der Bundeswehr angehören oder in ihm tätig werden, ist die Anzahl der potenziell zu überwachenden Personen von vornherein begrenzt. Im Gegensatz dazu bezieht sich die Aufklärungstätigkeit der übrigen Nachrichtendienste abstrakt auf einen unbegrenzten Personenkreis. Dies hat zur Folge, dass die potenziell von Maßnahmen des MAD Betroffenen eher damit rechnen müssen, beobachtet zu werden als die potenziell Betroffenen der anderen Nachrichtendienste. Dazu kommt, dass Soldaten bei der Einstellung darüber belehrt werden, dass sie sich einer Sicherheitsüberprüfung unterziehen müssen und in ihrer Laufbahn weitere Sicherheitsüberprüfungen notwendig werden können.³¹⁵ Das heißt, dass von Anfang an Berührungspunkte zum MAD existieren.

Neben dieser berufsbedingten Kenntnis des potenziellen Überwachtseins besteht ein weiterer Unterschied darin, dass Soldaten zur Verfassungstreue verpflichtet sind³¹⁶, was gem. Art. 33 Abs. 5 GG für sonstige Beamte (des Verteidigungsministeriums) ebenfalls gilt. Hierin unterscheiden sie sich von den Betroffenen der anderen Nachrichtendienste, soweit es sich nicht um Beamte handelt. Die Verfassungstreue und das Beobachtetwerden durch den MAD sind insoweit voneinander abhängig, als dass Mitarbeiter des Verteidigungsministeriums, bei denen nachweisbar ist, dass sie sich verfassungstreu verhalten, kein rechtmäßiges Ziel der Aufklärung durch den MAD sein können: Das bedeutet, wer seine Treueverpflichtung missachtet, muss damit rechnen, dass er Zielperson des MAD werden könnte. Die Beobachtungsobjekte der anderen Nachrichtendienste, die keiner strukturellen Treueverpflichtung unterliegen, stehen in keinem vergleichbaren Treueverhältnis zum Staat, das sie missachten könnten.

³¹⁵ Zum Beispiel, wenn ein Soldat im Ausland eingesetzt werden soll.

³¹⁶ Die Verfassungstreuepflicht gem. Art. 33 Abs. 5 GG wird analog angewandt, vgl. BVerwG, Beschluss vom 24.11.1987 – 1 WB 105/86.

(2) Auswirkungen auf die Kriterien

Vor diesem Hintergrund könnte man zunächst in Frage stellen, ob die Tätigkeit des MAD so *heimlich* ist wie die der anderen Nachrichtendienste. Dagegen spricht, dass Zielpersonen des MAD eher Kenntnis darüber haben, dass sie beobachtet werden könnten. Diese Kenntnis ändert allerdings an der Heimlichkeit der einzelnen Maßnahme im Ergebnis nichts: Wenn der MAD einzelne Maßnahmen mit Kenntnis der Betroffenen ausüben würde, wären sie sinnlos. Die oben beschriebene höhere Kenntnis bezieht sich daher auf die abstrakte Möglichkeit, nicht auf das konkrete Beobachtetwerden.

Da der Aufgabenbereich des MAD eng umgrenzt ist, können seine Maßnahmen von vornherein *nicht anlassunabhängig* jede Person treffen, was eingriffsmildernd einzustellen sein könnte. Im Ergebnis ist dies irrelevant, weil der MAD zur strategischen Überwachung – dem Hauptanwendungsfall der anlassunabhängigen Maßnahme – nicht befugt ist. Insofern besteht kein Unterschied zu den Verfassungsschutzbehörden.

Außerdem könnte man die Beobachtung durch den MAD als in Kauf genommenes „Berufsrisiko“ betrachten und dieses Risiko eingriffsmildernd einfließen lassen.³¹⁷ Dafür spricht, dass sie diesen Beruf trotz der oben beschriebenen Kenntnis von der abstrakten Überwachungsmöglichkeit und der Tatsache, dass die Soldaten und sonstige Beamten des Verteidigungsministeriums einer Treuepflicht unterliegen, ergriffen haben. Dagegen spricht, dass das Bundesverfassungsgericht ein „in Kauf zu nehmendes Berufsrisiko“ als eingriffsrelevanten Faktor in anderen Zusammenhängen nie erwähnt hat. Selbst wenn man ein „in Kauf nehmen“ als eingriffsmilderndes Kriterium annehmen wollte, würde sich das lediglich auf die abstrakte Möglichkeit, beobachtet zu werden, beziehen. Es bezöge sich nicht auf die konkreten, zu diesem Zeitpunkt nicht absehbaren Maßnahmen. Darüber hinaus könnte dieses Kriterium eingriffsintensivierend zu werten sein, sofern man es aus der Perspektive betrachtet, dass die Betroffenen dem Risiko im Zusammenhang mit ihrem grundrechtlich geschützten Berufsleben ausgesetzt sind. Überzeugender erscheint es, diesen Gedanken, wenn überhaupt, erst auf der Rechtfertigungsebene fruchtbar zu machen.

Die Kenntnis von der abstrakten Überwachungsmöglichkeit könnte dazu führen, dass die Angestellten des Verteidigungsministeriums aus Angst vor einer Maßnahme von der Ausübung eines ihrer Grundrechte wie beispielsweise der Meinungs- oder Versammlungsfreiheit *abgeschreckt* werden. Dieser Effekt wird dadurch verstärkt, dass die

³¹⁷ Gärditz schreibt im Zusammenhang mit einer Infiltration durch andere Nachrichtendienste, dass ein „Sozialbezug“ zum Nachrichtendienst in Form des Tätigwerdens in dem Nachrichtendienst eingriffsmildernd zu werten sei, Gärditz, EuGRZ 2018, 6, 16. Offen ist, ob ein solcher Sozialbezug zwischen Mitarbeitern des Verteidigungsministeriums und dem MAD schon wegen der Sicherheitsüberprüfung angenommen werden kann.

Beobachtung durch den MAD drastische *unmittelbare Folgen* für die gem. Art. 12 Abs. 1 GG geschützte Berufsfreiheit haben kann. Möglich ist beispielsweise die Eröffnung eines Disziplinarverfahrens³¹⁸, das sogar in der Entfernung vom Dienst enden kann³¹⁹.

(3) Höhere Eingriffsintensität

Das Bundesverfassungsgericht hatte bisher nicht über die Rechtsgrundlagen des MADG zu entscheiden. Aus diesem Grund ist offen, ob das Bundesverfassungsgericht die beschriebenen Differenzen zur Aufklärungstätigkeit von Verfassungsschutzbehörden und BND als eingriffserschwerende oder -mindernde Faktoren (Option 2 und 3) bzw. als für die Beurteilung der Eingriffsschwere irrelevant einordnen würden (Option 1).

Die wegen der Kenntnis von der abstrakten Überwachungsmöglichkeit entstehende Abschreckungswirkung für die Grundrechtsausübung und die unmittelbaren Folgen für die Berufsfreiheit sprechen dafür, die Intensität von Maßnahmen des Militärischen Abschirmdienstes höher einzustufen als vergleichbare Instrumente der anderen Nachrichtendienste (Option 2). Allerdings werden diese Nachteile durch die Verfassungstreuepflicht der Betroffenen ausgeglichen, weshalb die Eingriffsintensität der Maßnahmen des MAD denen der anderen Nachrichtendienste trotz der dargestellten Besonderheiten im Ergebnis entspricht (Option 1). Diese Überlegungen sind auf nachrichtendienstliche Tätigkeiten gegenüber sonstigen Beamten übertragbar.

5. Kontroll- Gesamtüberblick

In seiner Entscheidung zum Bayerischen Verfassungsschutzgesetz hat das Bundesverfassungsgericht erstmalig gefordert, dass die Nachrichtendienste das Zusammenwirken unterschiedlicher Maßnahmen beachten müssen.³²⁰ Außerdem hat es festgehalten, dass die Rechtskontrollorgane wissen müssen, welche Befugnisse gegenüber einem Betroffenen angewandt werden³²¹, mit anderen Worten: sie müssen über einen Kontroll-Gesamtüberblick verfügen.

³¹⁸ <https://www.dbwv.de/aktuelle-themen/newsbeitrag/fehlende-verfassungstreue-disziplinarverfahren-gegen-soldaten/> (abgerufen am 31.8.2024).

³¹⁹ <https://www.merkur.de/politik/bundeswehr-suspendiert-erstmal-reichsbuerger-vom-dienst-zr-10849581.html> (abgerufen am 31.8.2024).

³²⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 287 f.

³²¹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

a. Realität der additiven Anwendung nachrichtendienstlicher Mittel

Es ist möglich – und entspricht vermutlich der Praxis –, dass gegenüber einem Betroffenen mehrere nachrichtendienstliche Mittel angewandt werden.³²² Dies zeigt sich zum einen bereits darin, dass manche Befugnisse unter anderem den Zweck haben, andere Maßnahmen vorzubereiten: So erfährt die handelnde Behörde zum Beispiel durch den Einsatz von IMSI/IMEI-Catchern die Mobilfunknummer (und die Identität) einer Person, was es ihr ermöglicht, eine Telekommunikationsüberwachung durchzuführen.³²³ Bevor eine Wohnraumüberwachung beginnen kann, muss die Person zwangsläufig observiert worden sein, wie sonst sollte die Behörde einen Zeitraum abpassen können, in dem sich die Technik ungestört einbauen lässt? Befugnisse zur akustischen und optischen Überwachung außerhalb von Wohnungen werden bei und im Zusammenhang mit Observationen eingesetzt. Neben dieser funktionalen Verbindung einzelner Maßnahmen spricht die stufenartige Ausgestaltung der Befugnisse von leichten zu immer intensiveren Grundrechtseingriffen für eine additive Anwendung, jedenfalls in manchen Fällen. Wenn gegenüber einer Person sehr eingriffsintensive Maßnahmen eingesetzt werden, ist davon auszugehen, dass bereits weniger eingriffsintensive Maßnahmen eingesetzt wurden, um festzustellen, ob überhaupt Anhaltspunkte vorliegen, die den Einsatz der intensiveren Maßnahme rechtfertigen können. Darüber hinaus ist denkbar, dass Gespräche derselben Person mit Hilfe unterschiedlicher Maßnahmen belauscht werden, innerhalb der Wohnung durch eine Wohnraumüberwachung und außerhalb der Wohnung unter Einsatz technischer Hilfsmittel bei einer Observation.

Auch das Bundesverfassungsgericht geht von einer additiven Anwendung nachrichtendienstlicher Mittel aus.³²⁴

b. Additiver Grundrechtseingriff

Von einem additiven Grundrechtseingriff spricht man, wenn sich gleichzeitig mehrere Maßnahmen gegen einen Grundrechtsträger richten.³²⁵ Die gleichzeitig wirkenden Eingriffe müssen nicht dasselbe Grundrecht betreffen.³²⁶ Es ist möglich, dass ein oder gar mehrere Nachrichtendienste mit mehreren Maßnahmen gleichzeitig in die Grundrechte eines Betroffenen eingreifen. Häufig wird sogar der Schutzbereich desselben Grundrechts betroffen sein. Beispielsweise fällt sowohl die Observation als auch der

³²² Wetzling/Dietrich, Disproportionate use of commercially and publicly available data, S. 41.

³²³ Vgl. [Teil 1 B. III. 1.1.](#)

³²⁴ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 287.

³²⁵ Wissenschaftliche Dienste Deutscher Bundestag, Überwachungsgesamtrechnung 2022, S. 4.

³²⁶ Schwabenbauer, Hdb. des Polizeirechts, 842, 941 Rn. 342.; andere Ansicht Ruschmeier, Der additive Grundrechtseingriff, S. 260, Begründung, wieso es sich um dasselbe Grundrecht handeln muss und Darstellung anderer Auffassungen ebd. S. 136.

Einsatz von Vertrauensleuten und Verdeckten Ermittlern in den Schutzbereich des Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Werden diese Maßnahmen kombiniert angewandt, liegt ein additiver Grundrechtseingriff vor.

Soweit additiv in Grundrechte eingegriffen wird, müssen die Exekutivbehörden zur Wahrung der Verhältnismäßigkeit darauf achten, dass „das Ausmaß der Überwachung insgesamt beschränkt bleibt“. Das Bundesverfassungsgericht betont, dass gerade die additiven Grundrechtseingriffe ein „besonderes Gefährdungspotenzial“ für die Erstellung eines Persönlichkeitsprofils des Betroffenen bergen. Die Verantwortung für eine verhältnismäßige, kumulative Befugnisanwendung könne der Gesetzgeber der Behördenleitung übertragen.³²⁷

Seit dem Urteil zum bayerischen Verfassungsschutzgesetz (2022) sind nicht nur die Polizeibehörden, sondern auch die Nachrichtendienste dazu verpflichtet, zu beachten, inwieweit Maßnahmen additiv grundrechtsbelastend wirken.

c. Kontroll-Gesamtüberblick

Parallel zu dieser Verpflichtung der Nachrichtendienste soll ihr Kontrolleur das additive Überwachungs niveau einschätzen. So schreibt das Bundesverfassungsgericht in der Entscheidung zum bayerischen Verfassungsschutzgesetz, dass die Kontrollinstitution „jedenfalls alle Überwachungsmaßnahmen, denen eine Person durch eine Behörde ausgesetzt ist, in den Blick nehmen“ können muss. Diese Vorgabe sei zwingend, weil der Kontrolleur die Verhältnismäßigkeit einer Maßnahme der Nachrichtendienste vor dem Hintergrund der additiven Eingriffswirkung nur bewerten kann, wenn er weiß, welchen zusätzlichen Maßnahmen der Betroffene ausgesetzt ist.³²⁸ „In den Blick nehmen“ bedeutet dabei nicht, dass die Kontrolleure zwingend „überlappende“ Zuständigkeiten haben müssen; ausreichend ist, dass ein Kontrolleur auch dann Einsicht in Protokolle von Datenverarbeitungen nehmen kann, wenn er für die Kontrolle dieser Verarbeitung nicht zuständig war.³²⁹

Die Nachrichtendienstgesetze müssen deshalb eine Regelung enthalten, wonach der Kontrolleur³³⁰ alle Maßnahmen gegenüber einer Person überblicken kann³³¹, um sich so einen Kontroll-Gesamtüberblick verschaffen zu können.

³²⁷ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 287 f.; ähnlich BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 130.

³²⁸ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

³²⁹ *Sosna*, GSZ 2022, 245, 251.

³³⁰ Die Vorgaben sind in der Randnummer zur „aufsichtlichen Kontrolle“ enthalten, es handelt sich daher nicht um eine Spezifizierung der Vorabkontrolle.

³³¹ So auch *Bäcker*, Beschwerdeschrift G 10, S. 66.

aa) Maßnahmen einer Behörde

Grundsätzlich kommt es beim additiven Grundrechtseingriff nicht darauf an, welche staatliche Institution handelt.³³² Soll der Kontrolleur alle Maßnahmen kennen, denen der Betroffene additiv ausgesetzt ist, müsste die Kontrolle deshalb konsequenterweise – auch länderübergreifend – auf die Maßnahmen der anderen Nachrichtendienste und Sicherheitsbehörden erstreckt werden.³³³

Das Bundesverfassungsgericht hat jedoch leider eine engere Formulierung gewählt und festgelegt, dass es um alle Überwachungsmaßnahmen geht, denen eine Person „durch *eine* Behörde ausgesetzt ist“.

bb) Nicht jede Maßnahme

Das Bundesverfassungsgericht dürfte damit gemeint haben, dass der Kontrolleur in die Lage versetzt werden soll, bei der Beurteilung der Verhältnismäßigkeit potenziell alle weiteren Überwachungsmaßnahmen mitdenken zu können. Denn, so das Bundesverfassungsgericht, „das Ausmaß und die Rechtmäßigkeit einer Überwachung und die unter Umständen damit einhergehenden kumulativen Grundrechtseingriffe lassen sich nicht tragfähig beurteilen, wenn der Aufsichtsbehörde nur ein eingeschränkter Datenbestand zur Verfügung steht.“³³⁴ Der Kontrolleur soll demnach im Rahmen seiner stichprobenartigen Prüfung Zugriff auf alle Datenbestände einer Behörde haben.

d. Zwischenergebnis

Im Ergebnis müssen die Rechtskontrolleure gesetzlich ermächtigt werden, sich einen Kontroll-Gesamtüberblick darüber zu verschaffen, welche Maßnahmen der jeweilige Nachrichtendienst gegenüber einem Betroffenen anwendet.

6. Gleichwertigkeit bzw. Gerichtsähnlichkeit der Vorabkontrolle

Das Bundesverfassungsgericht hat in seiner Rechtsprechung zu Art. 10 Abs. 2 S. 2 GG etabliert, dass die Kontrolle durch die G 10-Kommission (oder ein Äquivalent) einer gerichtlichen Kontrolle „gleichwertig“ sein muss.³³⁵ Nach der neueren Rechtsprechung, in der das Bundesverfassungsgericht die Vorabkontrollen über den Anwen-

³³² *Ruschmeier*, Der additive Grundrechtseingriff, S. 150 ff.

³³³ „Die sog. additiven Grundrechtseingriffe, die ja nicht allein durch verschiedene Maßnahmen einer Behörde, sondern auch durch verschiedene Maßnahmen verschiedener Behörden vorliegen können, können ohnehin nur gemeinsam erkannt werden.“, *Sosna*, GSZ 2022, 245, 251.

³³⁴ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

³³⁵ Vgl. [Teil 2 A. III. 3 a. cc](#))

dungsbereich von Art. 10 Abs. 2 S. 2 GG hinaus ausgeweitet hat, muss die Vorabkontrolle zumindest „richterähnlich“ ausgestaltet sein. Die Begriffe der „gleichwertigen“ und „richterähnlichen“ Kontrolle sind identisch zu verstehen, denn bei beiden geht es darum, die Vergleichbarkeit mit der richterlichen Kontrolle abzubilden.

Für die Ausgestaltung eines verfassungskonformen Kontrolldesigns ist von zentraler Bedeutung, wie diese Begriffe auszulegen sind. Das Bundesverfassungsgericht selbst hat sie bereits detailliert (a.). Offen ist jedoch, welche Grenzen zu beachten sind, wenn aus der Gleichwertigkeit darüberhinausgehende, durch das Gericht nicht konkret benannte Anforderungen entnommen werden (b.).

a. Konkretisierung des Bundesverfassungsgerichts

Das Bundesverfassungsgericht betont, dass die Kontrolle durch eine unabhängige Stelle „materiell und verfahrensmäßig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll“ sein muss.³³⁶ Welche Aspekte für diese Gleichwertigkeit zwingend sind, hat das Bundesverfassungsgericht nicht abschließend spezifiziert.

Die Anforderungen an eine verfassungskonforme Ausgestaltung der Vorabkontrolle³³⁷ sollen fast alle die Gleichwertigkeit mit der gerichtlichen Kontrolle sicherstellen. Dies betrifft insbesondere die Unabhängigkeit der Kontrolleure, weil das Bundesverfassungsgericht insoweit mehrfach explizit den Vergleich zur richterlichen Unabhängigkeit gezogen hat.³³⁸ Dass die Vorgaben der Umsetzung einer richterähnlichen Kontrolle dienen, ergibt sich daraus, dass ihr Zweck darin besteht, den durch die Heimlichkeit bedingten Wegfall der Rechtsschutzmöglichkeiten Betroffener auszugleichen.³³⁹

Demgegenüber ist die Vorgabe, dass die Third Party Rule den Kontrollen nicht entgegengehalten werden kann³⁴⁰, nicht auf die Gerichtsähnlichkeit zurückzuführen. Gerichte gelten als „Dritte“ im Sinne der Third Party Rule, sodass ihnen gegenüber der Third Party Rule-Einwand erhoben werden kann.³⁴¹ Dass die Third Party Rule der

³³⁶ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69, 2 BvR 629/68 - 2 BvR 308/69 Rn. 77; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 275.

³³⁷ Vgl. [Teil 2 A. III. 1.](#)

³³⁸ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 77; BVerfG, Urteil v. 27.2.2008, 1 BvR 370/07 - Rn. 260; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 275.

³³⁹ Vgl. [Teil 2 A. I. 3. a.](#)

³⁴⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 293 ff.; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 224.

³⁴¹ Vgl. [Teil 2 A. III. 1. a. II.](#)

Kontrolle nicht entgegnet werden kann, ist daher nur realisierbar, wenn der Kontrolleur kein Gericht ist.

b. Grenzen weitergehender Vorgaben

Neben diesen in der Rechtsprechung detaillierten Ausprägungen der Gleichwertigkeit und Richterähnlichkeit stellt sich die Frage, welche Grenzen beachtet werden müssen, wenn aus ihnen weitere Anforderungen abgeleitet werden.

aa) Weitergehende Anforderungen in der Literatur

In der Literatur wird unter anderem vorgeschlagen, aus der Gleichwertigkeit abzuleiten, dass die Kontrolleure über vergleichbare fachliche Fähigkeiten wie Richter verfügen müssen, dass ihre Entscheidungen Rechtskraft entfalten, dass dagegen eine Berufungsmöglichkeit besteht und dass die Interessen des Betroffenen durch einen Betroffenenvertreter in das Verfahren der Vorabkontrolle eingebracht werden sollten.³⁴²

Darüber hinaus wird die Forderung nach „eigenständige[n] Aufklärungs- und Informationsbeschaffungsrechte[n]“ einzelner Mitglieder von Kontrollorganen auf die Gleichwertigkeit gestützt. Aus der Gleichwertigkeit ergebe sich zudem, dass die einzelnen Kontrolleure eine „persönliche richterliche Unabhängigkeit von innen heraus sicher[stellen] und mit Leben (...) füllen“ müssen. Nur so lasse sich verhindern, dass sie in „exekutive Handlungs- und Entscheidungslogiken“ verfallen, die entweder „unreflektiert und habitualisiert internalisiert ablaufen“ oder entstehen, weil die Kontrolleure sich als „Teil der Exekutive und entsprechend ausgerichteter Interessen empfinden“.³⁴³

bb) Grenzen

(1) Unterscheidung zwischen richterlicher und gerichtsähnlicher Kontrolle

Zunächst muss berücksichtigt werden, dass das Bundesverfassungsgericht eine Präferenz für die Kontrolle durch ein Gericht geäußert hat³⁴⁴, wegen der Besonderheiten der heimlichen Informationsbeschaffung aber eine richterähnliche Kontrolle zulässt³⁴⁵.

³⁴² Bantlin, G 10-Kommission, S. 158, 162 f.

³⁴³ Bezogen auf das gerichtsähnliche Kontrollorgan des Unabhängigen Kontrollrats *Fahrner*, GSZ 2023, 223, 225 f.

³⁴⁴ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214; *Bäcker*, Hdb. des Verfassungsrechts, 1715, 1754 Rn. 119.

³⁴⁵ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 224.

Die Gleichwertigkeit und Richterähnlichkeit kann deshalb nicht so weit ausgelegt werden, dass die Besonderheiten der nachrichtendienstlichen Arbeit keine Berücksichtigung mehr finden, denn dann hätte das Bundesverfassungsgericht gleich vorgeben können, dass ein Gericht die Rolle des Vorabkontrolleurs übernehmen soll.

Eine Besonderheit, die statt der richterlichen eine lediglich *richterähnliche* Kontrolle rechtfertigt, ergibt sich aus der notwendigen Geheimhaltung der nachrichtendienstlichen Arbeit. Dass in der Anordnung „sensible sowie voraussetzungsvolle Aufklärungsstrategien“ offengelegt werden, spricht nach Ansicht des Bundesverfassungsgerichts nicht gegen eine unabhängige Kontrolle, weil verfassungsgerichtlich nicht vorgegeben sei, dass die Kontrolle durch ein Gericht erfolgen muss.³⁴⁶

Im Umkehrschluss bedeutet das, dass die aus der Gerichtsähnlichkeit zusätzlich abgeleiteten Vorgaben die Geheimhaltungsbedürftigkeit nicht konterkarieren dürfen.

In Rahmen dieser Ausführungen verweist das Bundesverfassungsgericht auf wissenschaftliche Beiträge, in denen zusätzliche Probleme der gerichtlichen Kontrolle erörtert werden.³⁴⁷ Der Verweis auf diese Fundstellen wird so interpretiert, dass das Bundesverfassungsgericht die darin geäußerten Bedenken gegenüber gerichtlichen Kontrollen als Gründe für eine besondere, lediglich richterähnliche Kontrolle anerkennt. Würden diese Aspekte aus der „Richterähnlichkeit“ hergeleitet, hätte das Bundesverfassungsgericht gleich gerichtliche Kontrollen vorschreiben können.

In diesen vom Bundesverfassungsgericht zitierten Aufsätzen wird festgehalten, dass nachrichtendienstspezifisches Fachwissen der Kontrolleure für die Ausübung der Kontrolle unentbehrlich ist. Bei gerichtlichen Kontrollen könne zudem die Third Party Rule nicht gewahrt werden, weshalb die Leistungsfähigkeit der Nachrichtendienste sinke.³⁴⁸

Daher ergibt sich eine Grenze für die Ableitung weiterer Vorgaben aus der Gleichwertigkeit bzw. Richterähnlichkeit daraus, dass die Anforderungen erstens die Geheimhaltung nachrichtendienstlicher Informationen nicht gefährden dürfen, dass sie zweitens der Notwendigkeit spezifischen Fachwissens nicht widersprechen dürfen und dass drittens die Third Party Rule gewährleistet werden muss.

³⁴⁶ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 224 bzgl. der Geheimhaltungsbedenken mit Verweis auf Gärditz, EuGRZ 2018, 6, 18; Weisser, DöV 2014, 831, 835.

³⁴⁷ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 224.

³⁴⁸ Auf die Third Party Rule geht nur Gärditz ein, Gärditz, EuGRZ 2018, 6, 18; stellt zusätzlich auf den nicht leistbaren Mehraufwand durch die Gerichte ab, Weisser, DöV 2014, 831, 835.

(2) Regelungsspielraum des Gesetzgebers

Hinzu kommt, dass das Bundesverfassungsgericht dem Gesetzgeber einen Spielraum bei der Ausgestaltung der richterähnlichen und administrativen Kontrolle bewahren wollte.³⁴⁹ Da das Bundesverfassungsgericht selbst detaillierte Vorgaben formuliert hat³⁵⁰, ist bei der Herleitung weiterer Anforderungen aus den Formulierungen des Bundesverfassungsgerichts Zurückhaltung geboten, um den Spielraum des Gesetzgebers nicht vollständig aufzulösen.

Der Gestaltungsspielraum wird jedoch gewahrt, wenn durch zusätzliche Anforderungen lediglich die bereits durch das Bundesverfassungsgericht selbst formulierten Vorgaben ausdifferenziert werden. Wenn kein Zusammenhang zu den Vorgaben des Bundesverfassungsgerichts besteht, spricht das dafür, dass der Gestaltungsspielraum des Gesetzgebers zu sehr verengt wird.

(3) Zwischenergebnis

Angesichts der bereits detaillierten Vorgaben des Bundesverfassungsgerichts zur Ausgestaltung der unabhängigen Vorabkontrolle wird dafür plädiert, bei der Ableitung weiterer Vorgaben aus der Gleichwertigkeit bzw. Gerichtsähnlichkeit restriktiv vorzugehen.

7. Fazit der Rechtsprechungsanforderungen

Führt man die Ergebnisse der vorangegangenen Unterabschnitte zusammen, ergeben sich überblicksartig folgende Kontrollanforderungen der Rechtsprechung:

1. Schwer oder besonders schwer in die Grundrechte eingreifende Befugnisse sind einer richterlichen oder richterähnlichen unabhängigen Vorabkontrolle zu unterwerfen. Dieses Erfordernis greift bei der überwiegenden Mehrheit der nachrichtendienstlichen Instrumente.

2. Alle nachrichtendienstlichen Maßnahmen unterliegen der Datenschutzaufsicht.

3. Für die Vorabkontrolle und die laufende Kontrolle hat das Bundesverfassungsgericht aus der Verhältnismäßigkeit Anforderungen an ein verfassungskonformes Kontrolldesign abgeleitet.

4. Bei besonderer Kernbereichsrelevanz müssen spezielle Kernbereichsschutzvorkehrungen getroffen werden, teilweise muss eine unabhängige Stelle eingebunden werden.

³⁴⁹ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 282; auch in BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 224, 290 legt sich das Bundesverfassungsgericht nicht auf einen konkreten Kontrolleur fest.

³⁵⁰ Der Detailgrad der Rechtsprechung wird deutlich kritisiert, vgl. [Teil 2 A. III. 1.](#)

5. Die Kontrolleure müssen für den nach der neuesten Rechtsprechung erforderlichen Kontroll-Gesamtüberblick über alle Maßnahmen einer Behörde gegenüber der betroffenen Person Kenntnis haben können.

IV. Kritische Würdigung der Rechtsprechung

Die Positionen des Bundesverfassungsgerichts sind naturgemäß nicht unwidersprochen geblieben. Ziel dieses Abschnitts ist es, die häufigsten Kritikpunkte aufzugreifen. Der Fokus liegt auf ausgewählten, urteilsübergreifend relevanten Themen. Dabei wird zunächst überblicksartig dargestellt, wie sich die Diskussion zu unabhängigen Vorabkontrollen im Laufe der Jahre entwickelt hat (1.), bevor anschließend einzelne Aspekte vertieft erörtert werden (2.).

1. Entwicklung der Diskussion

Zunächst ist festzuhalten, dass die Nachrichtendienste schon lange tätig waren, bevor ihre Tätigkeit rechtlich angeleitet wurde. Für das Bundesamt für Verfassungsschutz gab es zwar bereits zu seiner Gründung 1950 mit dem BVerfSchG eine Rechtsgrundlage, die allerdings nur die Zusammenarbeit mit den Landesämtern für Verfassungsschutz und die Aufgaben des BfV regelte.³⁵¹ Erst vierzig Jahre später, 1990, wurde das BVerfSchG dann unter anderem um Befugnisnormen ergänzt.³⁵² Darin waren die nachrichtendienstlichen Mittel zwar nur exemplarisch benannt, immerhin wurden jedoch Tatbestandsvoraussetzungen für deren Einsatz und die anschließende Weiterverarbeitung normiert.³⁵³

³⁵¹ Das BVerfSchG v. 27.9.1950 hatte bei seiner Verkündung sechs Normen, vgl. BGBl I S. 1382; nach damaligem „Gesetzesverständnis“ habe die Aufgabenzuweisung die Befugnis zu Grundrechtseingriffen erfasst, Schenke/Graulich/Ruthig/Roth, Vorbem § 1 BVerfSchG Rn. 1.

³⁵² Art. 2 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 20.12.1990, BGBl I S. 2954, 2970 ff.

³⁵³ §§ 8 Abs. 2, 9, 10 ff. BVerfSchG in der Fassung v. Art. 2 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 20.12.1990, BGBl I S. 2954, 2970 ff.

Mit demselben Gesetz wurden 1990 erstmals Rechtsgrundlagen für den Bundesnachrichtendienst (BNDG)³⁵⁴ und den Militärischen Abschirmdienst (MADG)³⁵⁵ geschaffen, in denen zwar eigene Aufgaben formuliert waren, bezüglich der Befugnisse aber auf das BVerfSchG verwiesen wurde.³⁵⁶ Bis dahin war die Tätigkeit des BND auf Organisationserlasse gestützt und über eine Dienstanweisung angeleitet³⁵⁷, auch die Handlungen des MAD waren lediglich durch einen Erlass des Verteidigungsministers legitimiert³⁵⁸. Nur die Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses durch das 1968³⁵⁹ verkündete G 10 waren zu diesem Zeitpunkt schon mehr als 20 Jahre gesetzlich geregelt und von der G 10-Kommission kontrolliert worden. Obwohl es auf der Bundesebene seit 1950 ein – wenn auch nur schlankes – BVerfSchG gab, haben die Länder „nur zögernd“ Verfassungsschutzgesetze erlassen, die „bemerkenswerte Abweichungen“ aufwiesen.³⁶⁰ So wurde in Nordrhein-Westfalen beispielsweise erst 1994 ein Landesverfassungsschutzgesetz verabschiedet.³⁶¹

a. Notstandsverfassung, Einführung des G 10 und Abhörentscheidungen

Die ersten externen Rechtskontrolleure der Nachrichtendienste waren die G 10-Kommissionen.³⁶² Ihre Einführung hing mit den Verfassungsänderungen von 1968 unmittelbar zusammen: Im Rahmen der Notstandsverfassung wurden sowohl Art. 19 Abs. 4 GG als auch Art. 10 GG geändert. Fortan konnte eine gesetzliche Regelung für Ein-

³⁵⁴ Art. 3 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 20.12.1990, BGBl I S. 2977 ff.; Huber, NVwZ 2000, 393, 394; die Rechtsgrundlagen waren allerdings auf „Sachverhalte mit Inlandsbezug beschränkt (...). Für die sogenannte ‚Ausland-Ausland-Aufklärung‘ – also Sachverhalte ohne jedweden Inlandsbezug – beließ es der Gesetzgeber zunächst bei der Schaffung von Aufgabennonnen“, Aust, DöV 2020, 715, 716.

³⁵⁵ Art. 4 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 20.12.1990, BGBl I S. 2979 ff.; In der Wissenschaft wurde ausführlich diskutiert, ob Nachrichtendienste überhaupt einer Rechtsgrundlage bedürfen, vgl. insoweit der Überblick über die unterschiedlichen Positionen bei Rieger, ZRP 1985, 3.

³⁵⁶ Art. 3, 4 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 20.12.1990, BGBl I, S. 2977 ff.

³⁵⁷ Organisationserlasse 1955 und 1963, Dienstanweisung 1968, Friesenhahn, Kontrolle, 87, 93.

³⁵⁸ Der Erlass zur Gründung erfolgte 1956. „Das Bestreben, dem MAD (...) eine ausdrückliche gesetzliche Grundlage (...) zu verleihen, hatte sich zunächst weniger aus datenschutzrechtlichen Überlegungen ergeben als vielmehr aus dem skandalauslösenden, rechtswidrigen Einsatz von Abhörmitteln in elf Fällen während der Jahre 1972 bis 1977.“, Schenke/Graulich/Ruthig/Siems, § 1 MADG Rn. 1.

³⁵⁹ Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses v. 13.6.1967, BGBl I, S. 949.

³⁶⁰ Während das Hessische Verfassungsschutzgesetz 1980 weder Aufgaben noch Befugnisse regelte, enthielt das Verfassungsschutzgesetz in Bremen Voraussetzungen für den Einsatz nachrichtendienstlicher Mittel, Friesenhahn, Kontrolle, 87, 95.

³⁶¹ Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen, Nr. 5 v. 25.1.1995, S. 28 ff.

³⁶² Bartodziej, Hdb. des Recht der Nachrichtendienste, 1533, 1537.

griffe in Art. 10 GG unter bestimmten Voraussetzungen von der Benachrichtigung Betroffener absehen und den Rechtsweg ausschließen, wenn „an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt“. Kurz darauf wurde mit dem G 10 ein Gesetz verabschiedet, mit dem dies ermöglicht und die G 10-Kommission geschaffen wurde.³⁶³

Zu Beginn ihrer Tätigkeit wurde die G 10-Kommission des Bundes nachträglich über Beschränkungen informiert und konnte erst dann über die Rechtmäßigkeit von Anordnungen entscheiden. Weil der neue Bundesinnenminister Hans-Dietrich Genscher (FDP) das G 10 als Oppositionspolitiker jedoch kritisiert und „erbittert bekämpft“ hatte, wurden die Anordnungen ab seiner Amtszeit 1969 nicht mehr länger nur nachträglich, sondern fortan vorab genehmigt.³⁶⁴

1970 bestätigte das Bundesverfassungsgericht in der ersten Abhörentscheidung die Verfassungskonformität der Verfassungsänderungen und des G 10 und formulierte unter anderem Vorgaben für die Ausgestaltung der Kontrolle durch die G 10-Kommissionen.³⁶⁵ In der Literatur war diese Entscheidung hoch umstritten, allerdings bezog sich die Kritik hauptsächlich auf die Auslegung der Ewigkeitsklausel gem. Art. 79 Abs. 3 GG.³⁶⁶

An den Ausführungen des Bundesverfassungsgerichts zur G 10-Kommission wurde vor allem kritisiert, dass diese Kontrolle einer gerichtlichen Kontrolle nicht

³⁶³ Siebzehntes Gesetz zur Ergänzung des Grundgesetzes v. 24.6.1968, BGBl I S. 709 f.; Gesetz zur Beschränkung des Brief- Post- und Fernmeldegeheimnisses v. 13.8.1968, BGBl I S. 949.

³⁶⁴ Das sollte dem neuen Minister „die Anwendung des G 10 erleichtern“. 1978 wurde die vorherige Genehmigung dann auch gesetzlich vorgegeben, Arndt, G 10-Verfahren, 43, 53; vgl. [Teil 2 A. III. 3. a. bb\)](#)

³⁶⁵ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69; vgl. [Teil 2 A. III. 3. a. cc\).](#)

³⁶⁶ Vgl. z.B. Häberle, JZ 1971, 145, 149 ff.; Sachs/Pagenkopf, Art. 10 GG Rn. 51; Huber/Voßkuhle/Gusy, Art. 10 GG Rn. 97.

gleichwertig sei.³⁶⁷ Bis heute gibt es Stimmen, die fordern, den Rechtswegausschluss für nachrichtendienstliche Aktivitäten rückgängig zu machen.³⁶⁸

Außerdem wurde bemängelt, dass die Beschränkungsmaßnahmen nur einmalig, bei der Datenerhebung, kontrolliert wurden und die weitere Datenverarbeitung des Nachrichtendienstes aus dem Kontrollgegenstand ausgenommen war.³⁶⁹ Dem schloss sich das Bundesverfassungsgericht in der dritten Abhörentscheidung 1999 an: seitdem muss die Kontrolle „den *gesamten Prozess der Erfassung und Verwertung* der durch Maßnahmen nach dem G 10 erlangten Daten umfassen.“³⁷⁰

Obwohl das Bundesverfassungsgericht vorgegeben hat, dass das Kontrollorgan alle mit der „Vorbereitung, Entscheidung, Durchführung und Überwachung des Eingriffs in das Brief-, Post- und Fernmeldegeheimnis“ befassten „Organe“ kontrolliert und dass ihm Zugang zu allen erheblichen Unterlagen des Falles zu gewähren ist³⁷¹, gab es in der rechtswissenschaftlichen Literatur Meinungsverschiedenheiten zur Reichweite der Kontrollmittel, die sich darauf bezogen, wer zulässiger Adressat der Kontrollmittel sein kann.³⁷²

³⁶⁷ Sondervotum zu BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 der Bundesverfassungsrichter Geller, von Schlabrendorff, Rupp, Rn. 128; Riegel, § 5 G 10 Rn. 31; zweifelnd Gusy, NJW 1981, 1581, 1583; a.A. bspw. Kayzers, AöR 2004, 121, 135; Wischmeyer kritisiert die Vorgaben des Bundesverfassungsgerichts: „Die im Abhörurteil entwickelten Vorgaben waren allerdings – auch angesichts der aus den Besonderheiten der nachrichtendienstlichen Aufgabenerfüllung resultierenden Eigendynamik der Nachrichtendienste – von Anfang an unzureichend, um das Ziel eines gerichtsähnlichen »Ersatzverfahrens« zu erreichen; jedenfalls haben sie mit der Entwicklung der nachrichtendienstlichen Fähigkeiten nicht Schritt gehalten und sind aus heutiger Sicht klar ungenügend.“, Dreier/Brosius-Gersdorf/Wischmeyer, Art. 10 GG Rn. 98.

³⁶⁸ Deiseroth, ZRP 2013, 196; „Für den Ausschluss einer ähnlichen uneingeschränkten gerichtlichen Kontrolle von G 10-Maßnahmen in der Bundesrepublik ist daher kein Grund ersichtlich, zumal ursprünglich auch bei uns die richterliche Anordnung vorgesehen war (...)“, Riegel, § 5 G 10 Rn. 34; fordert dies jedenfalls, soweit die Nachrichtendienste „sich der Kriminalitätsabwehr widmen“, Graulich, Justizgewährung und Geheimdienste, 143, 159; schlägt auch die Verlagerung der G 10-Kontrolle auf Gerichte vor, Bartodziej, Hdb. des Rechts der Nachrichtendienste, 1533, 1604.

³⁶⁹ Kritisierte dies als „Schaffung kontrollfreier Räume“, Mangoldt/Klein/Starck/Gusy, 4. Auflage 1999, Art. 10 GG Rn. 99.

³⁷⁰ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 171; diese Maßgabe wurde 2001 einfach-rechtlich in § 15 Abs. 5 G 10 umgesetzt, Kayzers, AöR 2004, 121, 134.

³⁷¹ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 - Rn. 77.

³⁷² So kritisierte Schlink, dass die Kontrollinitiative durch eine Vorlage der Anordnung vom Kontrollierten ausgeht und dass die Kontrollmittel nur gegenüber der Exekutive, nicht aber gegenüber den verpflichteten Privaten (hier: der Post) geltend gemacht werden könnten, Schlink, Der Staat 1973, 85, 107; dieser Interpretation der Rechtslage widersprach beispielsweise Arndt, G 10-Verfahren, 43, 56.

b. Schaffung der Datenschutzbeauftragten und Meilenstein Volkszählungsurteil

Auf die G 10-Kommissionen als erste externe Rechtskontrollure der Nachrichtendienste folgten bald die Datenschutzbeauftragten, die einen breiteren Auftrag haben, deren Zuständigkeit sich aber auch auf die Kontrolle der Nachrichtendienste erstreckt.

Hessen war 1970 das erste Bundesland, in dem ein Datenschutzgesetz verabschiedet wurde, das unter anderem Kontrollen durch einen Datenschutzbeauftragten vorgab.³⁷³ Zwölf Jahre später war Hamburg dann das letzte Bundesland, in dem ein Landesdatenschutzgesetz erlassen wurde.³⁷⁴ Der erste BfDI, Hans Peter Bull, nahm 1978 in Folge der Verabschiedung des ersten Bundesdatenschutzgesetzes seine Tätigkeit auf.³⁷⁵

Zu diesem Zeitpunkt gab es außerhalb des G 10 allerdings noch keine gesetzliche Regelung für die Befugnisse der Nachrichtendienste des Bundes.³⁷⁶ Das wirkte sich auf potenzielle Kontrollen aus. Der BfDI mahnte daher 1981:

„Es genügt nicht, dass die Aufgabe gesetzlich zugewiesen oder geregelt ist; auch die jeweils ausgeübte Befugnis muss gesetzlich zugewiesen sein. Nur die Aufgabenumschreibung im Gesetz zu verlangen, käme einem Freibrief für praktisch unkontrollierbare Tätigkeit gleich, und dieser kann einer rechtsstaatlichen Verwaltung nicht zustehen.“³⁷⁷

Im Volkszählungsurteil vom 14.12.1983 stellte das Bundesverfassungsgericht dann klar, dass staatliche Datenverarbeitungen als Eingriffe in das (neu geschaffene) Recht auf informationelle Selbstbestimmung zwingend einer gesetzlichen Grundlage bedürfen.³⁷⁸ Zudem sei es für einen effektiven Schutz des RaiS von „erheblicher Bedeutung“, dass unabhängige Datenschutzbeauftragte an der Datenverwendung „beteiligt“ sind,

³⁷³ Gesetz- und Verordnungsblatt für das Land Hessen v. 12.10.1970, S. 625 ff.; Kauß, Der suspendierte Datenschutz, S. 91.

³⁷⁴ Kauß, Der suspendierte Datenschutz 1989, S. 104.

³⁷⁵ Gesetz zum Schutz von Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG), BGBl I v. 1.2.1977, S. 201, 209; <https://www.bfdi.bund.de/DE/DerBfDI/Inhalte/Datenschutzpfad/Geschichte-Datenschutz.html> (abgerufen am 31.8.2024).

³⁷⁶ Vgl. [Teil 2 A. IV. 1.](#)

³⁷⁷ Bull, Datenschutz, 133, 137 f.; kritisch auch Evers, NJW 1978, 1144, 1145; Friesenhahn stimmt zu, dass eine „Schwierigkeit einer jeden Kontrolle der Dienste“ darin besteht, „dass kein strikter Kontrollmaßstab besteht“, der aber der Ansicht ist, dass die nachrichtendienstlichen Mittel „auch nicht definierbar“ seien, Friesenhahn, Kontrolle, 87, 99.

³⁷⁸ BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83 - Rn. 149, 150 ff.; Schenke/Graulich/Ruthig/Siems, § 1 MADG Rn. 2.

weil automatische Datenverarbeitungen für Betroffene undurchsichtig seien und die Kontrolle dem „Interesse an vorgezogene[m] Rechtsschutz“ diene.³⁷⁹

Das Volkszählungsurteil begründet im Ergebnis einen grundsätzlich umfassenden Schutz personenbezogener Daten, der nicht nach einzelnen Erhebungsweisen oder besonderen Datenkategorien differenziert. Stattdessen soll die Schutzwürdigkeit von Daten durch die Art ihrer Verwendung bestimmt werden. Die Beteiligung unabhängiger Datenschutzbeauftragter ist in gleicher Weise – das heißt generell – vorgesehen.³⁸⁰

Wie eine verfassungsmäßige Beteiligung in diesem Sinne ausgestaltet sein muss, konkretisiert das Gericht im Volkszählungsurteil jedoch nicht. In der Literatur überwiegt die Auffassung, dass das Bundesverfassungsgericht den Datenschutzbeauftragten nur beispielhaft genannt hat und dass die institutionelle Ausgestaltung der Datenschutzkontrolle im Regelungsspielraum des Gesetzgebers verbleiben sollte.³⁸¹

Obwohl das Bundesverfassungsgericht deutlich formuliert hat, dass für staatliche Datenverarbeitungen eine Rechtsgrundlage notwendig ist, dauerte es weitere sieben Jahre, bis das BNDG und das MADG geschaffen und im BVerfSchG Befugnisnormen ergänzt wurden. Obwohl es nun jedenfalls Tatbestandsvoraussetzungen für den Einsatz nachrichtendienstlicher Mittel gab, wurde zu Recht unter anderem kritisiert, dass aus dem Gesetz nicht hervorging, welche nachrichtendienstlichen Mittel eingesetzt werden, da sie in § 8 Abs. 2 BVerfSchG rein exemplarisch benannt werden und ansonsten in einer nicht-öffentlichen Dienstanweisung konkretisiert sind.³⁸²

Dass noch heute viel diskutierte Problem, dass den Datenschutzbeauftragten als stärkste Kontrollergebnisfolge lediglich ein Beanstandungsrecht, aber keine abschließende Entscheidungskompetenz verliehen worden ist³⁸³ und die Kontrollmittel der Datenschutzbeauftragten nicht uneingeschränkt gelten³⁸⁴, wurde bereits damals diskutiert.

c. Konflikt zwischen dem BfDI und der G 10-Kommission

Wie die Kontrollkompetenzen der Datenschutzbeauftragten und der G 10-Kommissionen abzugrenzen sind, war von Beginn an umstritten: Nachdem der BfDI 1979 im

³⁷⁹ BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83 - Rn. 157.

³⁸⁰ *Denninger*, KJ 1985, 215, 220, 228.

³⁸¹ Dürig/Herzog/Scholz/*Di Fabio*, Art. 2 GG Rn. 184 m. w. Nachweisen; *Scholz/Pitschas*, Informationelle Selbstbestimmung, S. 47.

³⁸² *Geiger*, DVBl 1990, 748, 750; zum BNDG: Gesetzestext und Begründung zeichneten sich durch „apodiktische Kürze aus“, *Schenke/Graulich/Ruthig/Gusy*, Vorb § 1 BNDG Rn. 10.

³⁸³ Weil unter anderem deshalb die Kontrolle der Nachrichtendienste durch den BfDI nicht wirksam sei, schlug er einen Bundesbeauftragten für den Datenschutz „eigens für den Bereich der Geheimdienste vor“, *Geiger*, DVBl 1990, 748, 750 f.; a. A. *Kauß*, Der suspendierte Datenschutz, S. 406.

³⁸⁴ *Gusy*, Richterliche Kontrolle, 67, 90.

Anwendungsbereich von Art. 10 GG erstmalig Kontrollen durchgeführt hat, wurden ihm diese Kontrollen bereits 1980 verweigert.³⁸⁵ Damit einher ging eine Diskussion zwischen der G 10-Kommission und dem BfDI darüber, ob der G 10-Kommission in ihrem Zuständigkeitsbereich ein alleiniges Kontrollrecht zusteht.

Claus Arndt, Mitglied der G 10-Kommission, argumentierte damals, dass das G 10 gegenüber dem Bundesdatenschutzgesetz (BDSG) als *lex specialis* vorrangig anzuwenden sei und dass daher die Kontrolle der G 10-Kommission der des BfDI vorgehen müsse. Außerdem sei die G 10-Kommission auch für die Kontrolle des BfDI zuständig, soweit der BfDI G 10-Daten prüfe, eine solche „Doppel- und Querkontrolle zu konstituieren“ sei jedoch unvernünftig.³⁸⁶

Dem entgegnete Reinhard Riegel, Abteilungsleiter beim BfDI, dass die Kontrolle des BfDI im Anwendungsbereich des G 10 gesetzlich nicht ausgeschlossen sei, obwohl der Gesetzgeber die Prüfungskompetenz der parlamentarischen Kontrollkommission insoweit zugunsten der G 10-Kommission beschränkt habe. Demnach habe der Gesetzgeber Kontrollen durch den BfDI gerade nicht ausschließen wollen. Der BfDI sei zwar „an die Billigung einer Maßnahme durch die G 10-Kommission gebunden“, die Weiterverarbeitung der erhobenen Daten hingegen sei „voll nachprüfbar, ebenso die Einhaltung eventuell von der [Anm.: G 10-]Kommission gestellter Bedingungen“.³⁸⁷

Schließlich beendete der Gesetzgeber diesen Konflikt im Jahr 1990 zugunsten der G 10-Kommission, indem er die Zuständigkeit des BfDI insoweit gesetzlich ausschloss³⁸⁸, obwohl das Bundesverfassungsgericht in seiner zweiten Abhörentscheidung 1984 die Verfassungsmäßigkeit von § 3 G 10 auch damit begründet hat, dass eine Kontrolle durch „unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane (Kontrollkommission und Datenschutzbeauftragte)“ sichergestellt sei³⁸⁹. Die G 10-Kommission erhielt jedoch die Möglichkeit, den BfDI um Stellungnahmen zu bitten, was auf Seiten der Datenschutzkontrolleure als „Feigenblatt“ bewertet wurde.³⁹⁰

³⁸⁵ 3. Tätigkeitsbericht des BfDI 1980 v. 9.1.1981, BT/Drs. 9/93, S. 47 f., 55: „Zu einer Prüfung selbst ist es jedoch nicht gekommen, weil mir aufgrund einer Meinungsäußerung der G 10-Kommission (...) die Kompetenz für den Bereich der Telefonkontrolle abgesprochen wird. Die Kommission vertritt die Ansicht, sie sei in diesem Bereich zuständig (...).“; als „einen seit 1980 offenen Kompetenzstreit“ bezeichnet es der damalige Abteilungsleiter beim BfDI, Riegel, DöV 1985, 315.

³⁸⁶ Arndt, G 10-Verfahren, 43, 63.

³⁸⁷ Riegel, DöV 1985, 316 f.

³⁸⁸ § 24 Abs. 2 BDSG i. d. Fassung v. Art. 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 20.12.1990, BGBl I S. 2954, 2962 f., vgl. auch Bt-Drs. 11/4306, Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 6.4.1989, S. 48; kritisch Zöllner, Datenschutzbeauftragte im Verfassungssystem, S. 199, Gusy, Richterliche Kontrolle, 67, 90.

³⁸⁹ BVerfG, Beschluss vom 20.6.1984 - 1 BvR 1494/78 - Rn. 75; Riegel, ZRP 1987, 431, 434.

³⁹⁰ § 24 Abs. 2 S. 3 Nr. 1 BDSG a.F.; Riegel, § 8 G 10 Rn. 4a.

Darüber hinaus wurde diskutiert, ob die Kontrolle durch die Datenschutzbeauftragten als „gleichwertig“ zur gerichtlichen Kontrolle bewertet werden kann. Unter anderem mit Verweis darauf, dass die Datenschutzbeauftragten kein verbindliches Entscheidungsrecht haben, wurde dies zutreffend verneint.³⁹¹

d. Enthüllungen von Edward Snowden

„Das Potential der Nachrichtendienste hat (...) heute nur noch wenig zu tun mit dem von vor 60 Jahren (...). Während früher von vornherein nur spezifisch fokussierte, offensichtlich für die Ordnung insgesamt bedrohliche ‚Bestrebungen‘ beobachtet werden konnten, kann nun – je nach Befugnis, Ausstattung und Fähigkeit – theoretisch annähernd jede Bewegung jedes Bürgers rekonstruiert werden.“³⁹² Nie zuvor wurden das Ausmaß der Möglichkeiten zur umfassenden staatlichen Datenerhebung so deutlich wie durch die Enthüllungen von Edward Snowden 2013, die in den sog. „NSA-Skandal“ mündeten.³⁹³ Snowden, ehemaliger Mitarbeiter der US-amerikanischen National Security Agency (NSA), hatte damals die weltweite Überwachung der NSA und ihrer Partner in Großbritannien, Kanada, Australien und Neuseeland öffentlich gemacht.³⁹⁴ Demnach erheben und verarbeiten diese Nachrichtendienste „flächendeckend[d], vorsorglich anlasslo[s] und mehr oder weniger voraussetzungslo[s] (...) alle Telekommunikationsdaten, die für die für die Strafverfolgung oder Gefahrenprävention einschließ- lich einer Vorfeldaufklärung der Nachrichtendienste nützlich sein könnten.“³⁹⁵

Als Reaktion auf die Enthüllungen wurde im Bundestag am 11. Februar 2014 ein Untersuchungsausschuss eingesetzt, der unter anderem prüfen sollte, wie sich die Massenüberwachung der anderen Nachrichtendienste auf Deutschland auswirkt und inwiefern deutsche Behörden involviert sind.³⁹⁶ Ein Ergebnis der Arbeit des Untersuchungsausschusses war die Reform des BNDG und des PKGrG Ende 2016, in der unter anderem Rechtsgrundlagen für die strategische Überwachung von Ausländern im

³⁹¹ Zöllner, Datenschutzbeauftragte im Verfassungssystem, S. 196 f.; Bäumler, NVwZ 1988, 199, 200; a. A. offenbar Gusy, Richterliche Kontrolle, 67, 88.

³⁹² Masing, Nachrichtendienste, 3, 6 f.

³⁹³ Greenwald, NSA collecting phone records; Borgers, Zehn Jahre NSA-Affäre 2023; Heidebach, DöV 2015, 594, 593; weist aber darauf hin, dass es bereits seit der Echelon-Affäre 1998 bekannt war, dass die Five Eyes den internationalen Telekommunikationsverkehr überwachen, Petri, ZD 2013, 557.

³⁹⁴ Aust, DöV 2020, 715, 716.

³⁹⁵ Hans-Jürgen Papier, 5. Sitzung des 1. Untersuchungsausschusses der 18. Wahlperiode, Öffentliche Anhörung von Sachverständigen am 22.05.2014, Stenographisches Protokoll 5 I, S. 5; Bt.-Drs. 18/12850 v. 23.6.2017, Beschlussempfehlung und Bericht des 1. Untersuchungsausschusses gemäß Artikel 44 des Grundgesetzes, S. 36.

³⁹⁶ Bt.-Drs. 18/12850 v. 23.6.2017, Beschlussempfehlung und Bericht des 1. Untersuchungsausschusses gemäß Artikel 44 des Grundgesetzes, S. 41.

Ausland geschaffen und die parlamentarische Kontrolle der Nachrichtendienste ausgebaut wurden.³⁹⁷

e. Schaffung des Unabhängigen Gremiums

Außerdem wurde mit dieser Novelle des BNDG 2016 ein zusätzlicher Rechtskontrollleur etabliert, das Unabhängige Gremium.³⁹⁸ Das Gremium aus drei Mitgliedern und drei Stellvertretern sollte Anordnungen im Rahmen der strategischen Ausland-Fernmeldeüberwachung vorab³⁹⁹ kontrollieren und die Umsetzung von bestimmten Anordnungen stichprobenartig prüfen⁴⁰⁰.

Die Ausgestaltung des Unabhängigen Gremiums wurde von Beginn an kritisiert: nicht nachvollziehbar sei, dass nur Richter des Bundesgerichtshofs oder Anwälte am Bundesgerichtshof Mitglieder werden konnten (§ 16 Abs. 1 BNDG a.F.), aber keine Richter des Bundesverwaltungsgerichts.⁴⁰¹ Es ergäbe keinen Sinn, dass das Unabhängige Gremium beim Bundesgerichtshof in Karlsruhe angesiedelt werde anstatt in der Nähe der BND-Zentrale, die es kontrollieren soll.⁴⁰² Es sei „verfassungsrechtlich bedenklich“, dass das Unabhängige Gremium anders als die G 10-Kommission nicht über

³⁹⁷ Bt.-Drs. 18/12850 v. 23.6.2017, Beschlussempfehlung und Bericht des 1. Untersuchungsausschusses gemäß Artikel 44 des Grundgesetzes, S. 1388 f.; BGBl I v. 30.12.2016 S. 3346 ff.; in der Expertenanhörung des Untersuchungsausschusses war das Fehlen einer solchen Rechtsgrundlage deutlich kritisiert worden, vgl. *Matthias Bäcker* in der 5. Sitzung des 1. Untersuchungsausschusses der 18. Wahlperiode, Öffentliche Anhörung von Sachverständigen am 22.5.2014, Stenographisches Protokoll 5 I, S. 15: „Das bedeutet, dass das Recht dieser Auslandsaufklärung eigentlich keinerlei Grenzen setzt. In welchem Ausmaß der Bundesnachrichtendienst Telekommunikationsdaten im Ausland erhebt, bevorratet und auch weiterübermittelt, ist wesentlich nicht vom Recht angeleitet, sondern hängt ab von ethischen Erwägungen der Mitarbeiter des Bundesnachrichtendienstes und im Übrigen von den personellen und technischen Ressourcen.“

³⁹⁸ BGBl I v. 30.12.2016, S. 3346, 3350.

³⁹⁹ Denkbar ist, dass die Anordnung häufig nachträglich kontrolliert wurden, weil sich das Gremium nach § 16 Abs. 4 S. 1 BNDG a.F. nur „mindestens alle drei Monate“ treffen musste, was zu wenig ist, *Schenke/Graulich/Ruthig/Dietrich*, § 16 BNDG Rn. 12.

⁴⁰⁰ §§ 16 Abs. 1, 15 Abs. 3, 9 Abs. 4, 5, § 10 Abs. 3 S. 2 BNDG a.F.; *Gärditz*, DVBl 2017, 525, 531.

⁴⁰¹ *Gärditz*, DVBl 2017, 525, 531; „obwohl es bei der Routineaufklärung noch viel weniger schwerpunktmäßig um strafrechtliche Sachverhalte geht als bei der G 10-Aufklärung“, *Bartodziej*, Hdb. des Rechts der Nachrichtendienste, 1533, 1605; *Schenke/Graulich/Ruthig/Dietrich*, § 1 BNDG Rn. 5; es hätte „sachlich näher gelegen“ diese Kontrolle dem sechsten Senat des Bundesverwaltungsgerichts zu übertragen, *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 183; kritisiert, dass die Richter von der Bundesregierung ernannt und die Bundesanwälte von ihren Weisungen abhängig sei, *Steinke*, Die dunklen Geheimdienstfürsten.

⁴⁰² *Gärditz*, DVBl 2017, 525, 531.

Kontrollmittel, wie Auskunfts-, Einsichts- und Zugangsrechte verfüge.⁴⁰³ Im Gegensatz zur G 10-Kommission prüfe das Unabhängige Gremium in der Regel keine Suchbegriffe, außer Suchbegriffe, die sich auf Einrichtungen der Europäischen Union oder öffentliche Stellen der Mitgliedsstaaten beziehen.⁴⁰⁴ Die „Qualität“ der Kontrolle durch das Unabhängige Gremium sei somit insgesamt geringer als die der G 10-Kommission.⁴⁰⁵

Dass mit dem Unabhängigen Gremium ein neuer Kontrolleur geschaffen werde, obwohl diese Aufgabe der G 10-Kommission hätte übertragen werden können, führe zu einer „dysfunktional[en]“ weiteren „Vermehrung der Kontrollorgane“.⁴⁰⁶

f. Entscheidung zur strategischen Ausland-Fernmeldeaufklärung

In seinem Urteil zur strategischen Ausland-Fernmeldeaufklärung forderte das Bundesverfassungsgericht 2020 eine Professionalisierung der Rechtskontrolle und formulierte detaillierte Vorgaben für die Ausgestaltung des Kontrolldesigns.⁴⁰⁷ Für diese Entscheidung erfuhr das Bundesverfassungsgericht sowohl Lob⁴⁰⁸ als auch Widerspruch. So wird beispielsweise als „begrüßenswert“ erachtet, dass es „die organisatorischen Anforderungen deutlich nachgeschärft hat“.⁴⁰⁹

Andere kritisieren jedoch den Detailgrad der aus dem Verhältnismäßigkeitsgrundsatz abgeleiteten Vorgaben.⁴¹⁰ Darüber hinaus sei nicht nachvollziehbar, wieso das Bundesverfassungsgericht sich nur an dem britischen Kontrolldesign orientiere, zu dem es

⁴⁰³ Schenke/Graulich/Ruthig/Dietrich, § 16 BNDG Rn. 2; Vogt, Strategische Auslandstelekommunikationsüberwachung, S. 184; Huber, ZRP 2016, 162, 165; Kritik daran äußerten auch die Mitglieder des Gremiums, Leyendecker/Pinkert, BND behindert Kontrollgremium.

⁴⁰⁴ Marxsen, DöV 2018, 218, 225.

⁴⁰⁵ Vogt, Strategische Auslandstelekommunikationsüberwachung, S. 184; Marxsen, DöV 2018, 218, 224; der „Kontrollrahmen“ sei im Vergleich zur G 10-Kommission „sehr restriktiv gefasst“, Bäcker, Stellungnahme zu einem Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des BND, S. 16.

⁴⁰⁶ Gärditz, DVBl 2017, 525, 532; ähnlich Bäcker, Stellungnahme zu einem Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des BND, S. 16 f.; Schenke/Graulich/Ruthig/Dietrich, § 16 BNDG Rn. 1; a.A. Vogt, Strategische Auslandstelekommunikationsüberwachung, S. 182; Schneider, Fernmeldegeheimnis, S. 320.

⁴⁰⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 324, 274 ff., vgl. [Teil 2 A. III. 1. b.](#)

⁴⁰⁸ Das Urteil sei „in seiner Argumentation gut nachvollziehbar“, Petri, ZD 2020, 409, 412; „Das Urteil überzeugt (...)“, Aust, DöV 2020, 715, 723 f.

⁴⁰⁹ Dass das Bundesverfassungsgericht bis dahin „über lange Zeit nur zurückhaltende Vorgaben“ gemacht hätte, „erstaun[e]“, Dreier/Brosius-Gersdorf/Wischmeyer, Art. 10 GG Rn. 98.

⁴¹⁰ „Es fällt schwer, solche Details – mögen sie auch rechtspolitisch klug sein – als Konsequenz der Verhältnismäßigkeit auszuflaggen. Pflichtschuldige Hinweise auf die Gestaltungsspielräume des Gesetzgebers nehmen daneben beinahe satirischen Charakter an.“, Gärditz, JZ 2020, 825, 833; „Mikromaßgaben“, Dietrich, GSZ 2020, 174, 181; Muckel, JA 2020, 631, 635; Barczak, KritV 2021, 91, 125 und Barczak, BayVbl 2020, 685, 691; Vogt, Strategische Auslandstelekommunikationsüberwachung, S. 535; a. A. z.B. Aust, DöV 2020, 715, 721.

in der Mündlichen Verhandlung sogar einen Sachverständigen angehört habe, die Kontrollkonzepte anderer Staaten trotz „gute[r] Gründe“ für ihre Beachtung bei seinen Überlegungen jedoch außen vorlasse.⁴¹¹ Außerdem wird kritisiert, dass das Bundesverfassungsgericht für den Wegfall der Geltendmachung von Betroffenenrechten keinen Ersatz fordert und dass das Verfahren damit „konstitutiv defizitär“ bleibe.⁴¹²

Ende 2021 löste der Gesetzgeber das Unabhängige Gremium auf und ersetzte es durch den neu geschaffenen UKRat.⁴¹³

g. Entscheidung zum Bayerischen Verfassungsschutzgesetz

Im April 2022 entschied das Bundesverfassungsgericht in seinem Urteil zum Bayerischen Verfassungsschutzgesetz dann unter anderem, dass der Einsatz von eingriffsintensiven nachrichtendienstlichen Maßnahmen zukünftig vorab durch einen unabhängigen Kontrolleur genehmigt werden muss.⁴¹⁴ Vereinzelt wird angemerkt, das Bundesverfassungsgericht spreche in dieser Entscheidung anders als in der zur strategischen Ausland-Fernmeldeaufklärung nicht mehr von gerichtsähnlich unabhängigen, sondern nur noch von unabhängigen Kontrolleuren, woraus abgeleitet wird, dass der Gesetzgeber einen größeren Gestaltungsspielraum habe, weil die Kontrollen „nicht zwingend gerichtsähnlich“ erfolgen müssen.⁴¹⁵ Andere betonen, die Vorgaben zum Kontrolldesign seien in beiden Entscheidungen „in der Sache parallel formuliert“.⁴¹⁶ Dass auch die Nutzung von Vertrauenspersonen zukünftig der unabhängigen Rechtskontrolle unterliegt und das Bundesverfassungsgericht sich insoweit den Geheimhaltungsbedenken

⁴¹¹ Dietrich, GSZ 2020, 173, 181; deutlich: „Das BVerfG hat hier schlicht Anforderungen abgeschrieben, die das britische Recht für das Investigatory Powers Tribunal normiert hat (Schedule 3 zu Sec. 65 ff. Regulation of Investigatory Powers Act 2000). Inspirationsbeflügelte Prozessrechtsvergleiche als Quelle der Verfassungsauslegung? Hier vergreift sich der Senat gründlich, zumal das britische Kontrollmodell, das in der Tat bislang am besten zu funktionieren scheint, schon dort pragmatisches Design des einfachen Gesetzgebers und zudem unlösbar mit grundlegend abweichenden Justiztraditionen sowie darin eingeschriebenen Staatsbildern verflochten ist (...)“, Gärditz, JZ 2020, 825, 833; Huber kritisiert einen Mangel an „Rechtstatsachenforschung“, weil das Bundesverfassungsgericht – entsprechend dem britischen Modell – nicht vorgegeben hat, dass die Leitungsebene der Nachrichtendienste in die Kontrolltätigkeit eingebunden wird, obwohl sich dies bei der G 10-Kommission bewährt habe, Huber, NVwZ-Beilage 2020, 3, 9.

⁴¹² Dreier/Brosius/Gersdorf/Wischmeyer, Art. 10 GG Rn. 98; so auch Vogt, Strategische Auslandstelekommunikationsüberwachung, S. 533.

⁴¹³ Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 19. April 2021, BGBl. I v. 21.4.2021, S. 771.

⁴¹⁴ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214.

⁴¹⁵ Bantlin/Graulich, GSZ 2023, 179, 182.

⁴¹⁶ Gärditz, GSZ 2022, 161, 170; Ogorek, NJW 2022, 1570, 1572.

der Exekutive nicht angeschlossen hat, wird positiv bewertet.⁴¹⁷ Kritisiert wird wie bereits in Bezug auf die Entscheidung zur strategischen Ausland-Fernmeldeüberwachung, dass die Vorgaben aus dem Verhältnismäßigkeitsgrundsatz abgeleitet werden und dass damit die in den Grundrechten „enthaltenen abgrenzbaren Schutzbereiche mit unterschiedlichen Schutzfunktionen und Schranken“ in einer „übergreifenden Verhältnismäßigkeitsprüfung“ aufgelöst würden.⁴¹⁸ Das führe dazu, dass die in der Verfassung explizit vorgegebenen Richtervorbehalte letztlich nur noch „bloß[e] Regelbeispiel[e]“ seien.⁴¹⁹

2. Kritikwürdige Aspekte

Überlegungen dazu, in welchen Aspekten die Rechtsprechung des Bundesverfassungsgerichts nicht überzeugt, sind Gegenstand des folgenden Abschnitts.

a. Fokussierung auf Vorabkontrollen

In der Rechtsprechung des Bundesverfassungsgerichts zum Nachrichtendienstrecht wird deutlich, dass das Bundesverfassungsgericht die Vorabkontrolle als wichtigsten Pfeiler des Grundrechtsschutzes durch Verfahren erachtet (aa)). Das ist wegen der mit der ex ante-Kontrolle verbundenen Vorteile grundsätzlich begrüßenswert (bb)). Die Erwartungen, die das Bundesverfassungsgericht an Kontrollen formuliert, kann die Vorabkontrolle jedoch nicht vollständig einlösen (cc), dd)). Insoweit überzeugt die Fokussierung auf die Vorabkontrolle nicht (ee)).

aa) Hervorgehobene Bedeutung der Vorabkontrolle

Zu Recht wird festgestellt, dass das Bundesverfassungsgericht „dem Richtervorbehalt eine zentrale Stellung bei der prozeduralen Dimension der Wahrung der Grundrechte der Betroffenen gegenüber staatlichen Informationserhebungen und -verarbeitungen zugewiesen hat“.⁴²⁰ So gilt beispielsweise für alle heimlichen, eingriffsintensiven Datenverarbeitungen, dass sie der Vorabkontrolle bedürfen,⁴²¹ egal ob die Polizei oder ein Nachrichtendienst tätig werden⁴²². Dabei hat das Bundesverfassungsgericht zwar eine

⁴¹⁷ Ogorek, NJW 2022, 1570, 1572.

⁴¹⁸ Gärditz, GSZ 2022, 161, 169 f.

⁴¹⁹ Gärditz, GSZ 2022, 161, 169 f.

⁴²⁰ Fahrner, GSZ 2023, 223, 224.

⁴²¹ Bäcker, Hdb. des Verfassungsrechts, 1715, 1754 Rn. 119.

⁴²² BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 117 f.; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214.

Präferenz für gerichtliche Kontrollen ausgedrückt, die Prüfung durch gerichtsähnliche Gremien aber ausdrücklich zugelassen.⁴²³

Betrachtet man die Rechtsprechung zum Nachrichtendienstrecht, wird deutlich, dass sich das Bundesverfassungsgericht der ex ante-Kontrolle durchweg detaillierter widmet als der laufenden und nachträglichen Kontrolle: In der ersten Abhörentscheidung, in der es die Vorgaben für die Kontrolle gem. Art. 10 Abs. 2 S. 2 GG formuliert,⁴²⁴ äußert es sich gar nicht zur laufenden Kontrolle. Selbst im für den Datenschutz konstitutiven Volkszählungsurteil sind die Ausführungen zur Datenschutzkontrolle eher kurz und prägnant, denn detailliert: an der Datenverarbeitung müssten unabhängige Datenschutzbeauftragte „beteiligt“ werden, weil automatische Datenverarbeitungen für den Betroffenen undurchsichtig seien und die Kontrolle dem Interesse an „vorgezogene[m] Rechtsschutz“ diene.⁴²⁵ In der zweiten Abhörentscheidung, in der das Bundesverfassungsgericht bei der Überprüfung der Normen zur strategischen Überwachung auf Prüfungsergebnisse des BfDI Bezug nimmt⁴²⁶, erwähnt es ebenfalls lediglich, dass neben der G 10-Kommission auch die Datenschutzbeauftragten Kontrollen sicherstellen.⁴²⁷ In der dritten Abhörentscheidung stellt das Bundesverfassungsgericht dann heraus, dass die G 10-Kommission nicht nur für die Genehmigung und die Entscheidung über Benachrichtigung Betroffener zuständig ist, sondern dass die Kontrolle „den gesamten Prozess der Erfassung und Verwertung der Daten“ umfasst.⁴²⁸ Die Entscheidung zur Online-Durchsuchung enthält detaillierte Vorgaben zur Vorabkontrolle bei eingriffsintensiven Maßnahmen außerhalb des Anwendungsbereichs von Art. 10 GG, unter anderem zum zuständigen Kontrolleur und dem Kontrollzeitpunkt⁴²⁹; demgegenüber wird die laufende Kontrolle nicht erwähnt. Erst in der Entscheidung zur Antiterrordatei von Polizei und Nachrichtendiensten entwickelt das Bundesverfassungsgericht Maßstäbe für die verfassungskonforme Ausgestaltung der Datenschutzkontrollen bei Sicherheitsbehörden und legt unter anderem fest, dass die Datenschutzaufsicht mit wirksamen Befugnissen auszustatten ist und dass alle Datenverarbeitungen protokolliert werden und in „praktikabel auswertbarer Weise zur Verfügung gestellt

⁴²³ Vgl. [Teil 2 A. III. 6.](#)

⁴²⁴ BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 - Rn. 77.

⁴²⁵ BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83 - Rn. 157.

⁴²⁶ BVerfG, Beschluss v. 20.6.1984 - 1 BvR 1494/78 - Rn. 69; *Riegel*, DöV 1985, 316.

⁴²⁷ BVerfG, Beschluss v. 20.6.1984 - 1 BvR 1494/78 - Rn. 75.

⁴²⁸ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 171, 302.

⁴²⁹ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 257 ff.

werden müssen“.⁴³⁰ Der Fokus auf die Vorabkontrolle ist auch in den aktuellsten Entscheidungen erkennbar: Im Urteil zur strategischen Ausland-Fernmeldeaufklärung des BND äußert sich das Bundesverfassungsgericht insgesamt detailliert zur Ausgestaltung der Kontrolle, formuliert die Vorgaben zur gerichtsähnlichen Kontrolle aber deutlich präziser.⁴³¹ Auch im Urteil zum bayerischen Verfassungsschutzgesetz führt das Bundesverfassungsgericht über einen längeren Textabschnitt aus, dass für alle eingriffsintensiven Maßnahmen unabhängige Vorabkontrollen eingeführt werden müssen⁴³², der laufende Kontrolle durch die Datenschutzbeauftragten widmet es hingegen nur eine Randnummer.⁴³³

bb) Vorteile und Erwartungen

Die Kontrolle vor Vollzug der Maßnahme hat den entscheidenden Vorteil, dass ungerechtfertigte Grundrechtseingriffe von vornherein vermieden werden können und eine Rechtsverletzung erst gar nicht eintritt.⁴³⁴

Das Bundesverfassungsgericht erachtet die Rechtskontrolle im Allgemeinen als erforderlich, um den Wegfall des subjektiven Rechtsschutzes gegen heimliche Maßnahmen zu kompensieren: Dass eingriffsintensive nachrichtendienstliche Maßnahmen von einer unabhängigen Stelle kontrolliert werden, sei besonders wichtig, weil die Betroffenen mangels Kenntnis von der heimlichen Maßnahme nicht die Möglichkeit haben, sich vorab dagegen zu wehren und sie auch im Nachhinein in der Regel nichts davon erfahren. Deshalb bleibt ihnen nicht nur der vorherige, sondern auch der nachträgliche Rechtsschutz verwehrt. Dieses rechtsstaatliche Defizit zu kompensieren, ist ein Ziel unabhängiger Kontrollen.⁴³⁵

Zudem soll die Vorabkontrolle nach der Auffassung des Bundesverfassungsgerichts dazu dienen, die Weite nachrichtendienstlicher Befugnisnormen auszugleichen.⁴³⁶ Bei der strategischen Ausland-Fernmeldeaufklärung des BND sollen die Kontrollen die

⁴³⁰ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 204, 207 f., 217; obwohl der Senat diese Anforderungen im Urteilstext nicht im Sinne eines *orbiter dictum* ausdrücklich auf sonstige nachrichtendienstliche Datenverarbeitungen erstreckt, gelten diese Bedingungen auch bei der Anwendung nachrichtendienstlicher Mittel. Wegen der Vergleichbarkeit der Verarbeitungssituation ist diese Rechtsprechung auf sämtliche heimliche Datenverarbeitungen durch Nachrichtendienste übertragbar, a. A. Gärditz, der davon ausgeht, dass die Anforderungen an den Einsatz geheimer Mittel durch die Nachrichtendienste insoweit „nur touchiert“ wurden, *Gärditz*, JZ 2020, 825, 834.

⁴³¹ Insoweit gibt es beispielsweise den Kontrollgegenstand und eine hochkarätige Besetzung vor, BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 272 ff., 275 ff., 278, 286.

⁴³² BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214 - 224.

⁴³³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

⁴³⁴ *Bantlin*, G 10-Kommission, S. 99.

⁴³⁵ Vgl. [Teil 2 A. I. 3. a.](#)

⁴³⁶ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 213.

„im Wesentlichen nur finale“ Gestaltung der Rechtsgrundlagen „verfahrensmäßig“ strukturieren und ihre „Handhabung“ sichern.⁴³⁷

cc) Zweifel an der Kompensation der Heimlichkeit durch Vorabkontrollen

Sowohl in der Literatur als auch von Seiten der Kontrolleure selbst werden Zweifel daran geäußert, dass die Vorabkontrolle die aus der Heimlichkeit der Maßnahme resultierenden Rechtsschutznachteile für Betroffene kompensieren kann.

Im Gegensatz zum Bundesverfassungsgericht gehen manche Stimmen in der Literatur davon aus, dass Richtervorbehalte dahingehend überhaupt nicht kompensierend wirken können.⁴³⁸ Andere weisen zu Recht darauf hin, dass der Betroffene im Vorabkontrollverfahren nicht gehört wird und der Kontrolleur die Entscheidung daher auf der Grundlage einer von der antragsstellenden Behörde formulierten, „selektiven Darstellung“ des Sachverhalts treffen muss, in der „Einwände des Betroffenen“ nicht vorkommen.⁴³⁹ Aus diesem Grund könne die Vorabkontrolle das Defizit im subjektiven Rechtsschutz zwar „abmildern, nicht aber beheben“.⁴⁴⁰ Diese Überlegungen sind auf begleitende und auf nachträgliche Kontrollen übertragbar, soweit der Betroffene nicht eingebunden ist.

Das ehemalige Mitglied des GeKons, Elisabeth Steiner, bekräftigt diese grundsätzlichen Bedenken in ihrem Resümee zur bisherigen Kontrolltätigkeit des GeKon, indem sie feststellt, „dass die Perspektive der durch die Umsetzung der Aufklärungsmaßnahmen konkret in ihren Grundrechten Betroffenen“ sich „im Rahmen der Vorabkontrolle häufig nur in sehr abstrakter Form“ abbilde. Weiter führt sie aus:

„Die vom Bundesverfassungsgericht bereits auf der Ebene der Vorabkontrolle angestrebte Prüfungstiefe nach Art einer gerichtlichen Einzelfallkontrolle lässt sich dort nicht erzielen. Erst im Zuge einer ex-post-

⁴³⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 273; vgl. [Teil 2 A. I. 3. b.](#)

⁴³⁸ Schwabenbauer, Heimliche Grundrechtseingriffe, S. 325 ff.

⁴³⁹ Bäcker, Kriminalpräventionsrecht, S. 153 f., so auch Bonin, Grundrechtsschutz, S. 279.

⁴⁴⁰ Bäcker, Kriminalpräventionsrecht, S. 153, der auf S. 154 richtigerweise davor warnt, wie u.a. das Bundesverfassungsgericht in BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 254 von einer „Repräsentation“ des Betroffenen zu sprechen, weil das Gericht in „Äquidistanz zu Behörde und Betroffenen“ stehe und „allein Sachwalter des Rechts“ sei; ebenso Bonin, Grundrechtsschutz, S. 286 f.; neben dem „Grundsatz der Allseitigkeit des Gehörs“ sei damit auch die „Neutralität im Sinne einer prozessualen Waffengleichheit“ beeinträchtigt, schreibt Gusy, der aber darauf hinweist, dass das fehlende rechtliche Gehör „(...) kein Mangel, sondern geradezu der Sinn des Verfahrens [der Vorabkontrolle]“ sei, der Richtervorbehalt sei „eine Art externalisierter Selbstkontrolle der Verwaltung“, Gusy, GA 2003, 672, 678.

*Kontrolle durch das administrative Kontrollorgan wird die Frage näher beleuchtet, ob der konkret zur Datenerhebung in einem oder mehreren Telekommunikationsnetzen gesteuerte Suchbegriff, die Auswahl des infiltrierten IT-Systems und der Umfang der Datenerhebung daraus für das Aufklärungsanliegen geeignet, erforderlich und verhältnismäßig im engeren Sinne war.*⁴⁴¹

Das bedeutet, dass der Vorabkontrolleur jedenfalls bei Maßnahmen der strategischen Ausland-Fernmeldeaufklärung und bei Eingriffen in informationstechnische Systeme von Ausländern im Ausland zum Zeitpunkt der Genehmigungsentscheidung in der Regel⁴⁴² die Einhaltung von Betroffenenrechten noch gar nicht prüfen kann, weil die dafür notwendigen Informationen fehlen. Das Problem betrifft jedoch nicht nur die genannten Maßnahmen des BND, sondern gilt immer dann, wenn eine Maßnahme nicht gezielt gegen Personen eingesetzt wird. Wenn das BfV beispielsweise eine Vertrauensperson gegen eine Bestrebung – und nicht gezielt gegen bestimmte Personen – einsetzt, muss die Verhältnismäßigkeitsprüfung ebenfalls abstrakt bleiben.

Weitergehende Offenlegungspflichten der Nachrichtendienste gegenüber ihren Vorabkontrolleur können dieses Problem nicht lösen, weil auch die Nachrichtendienste zum Zeitpunkt der Anordnung noch nicht über diese Informationen verfügen.

Die Perspektive der Betroffenen kann daher immer nur dann kompensierend berücksichtigt werden, wenn die Betroffenen zum Zeitpunkt der Genehmigung bekannt sind. Wenn der Betroffene nicht bekannt ist, kann der Vorabkontrolleur den Wegfall seines Rechtsschutzes auch nicht kompensieren.

dd) Zweifel an der Kompensation weiter Befugnisse

Darüber hinaus werden Zweifel daran geäußert, dass die Vorabkontrolle weite, unbestimmte Befugnisnormen kompensieren könne.

⁴⁴¹ Steiner, GSZ 2023, 124, 130; ähnlich bereits Gärditz, der auf die „geringer[e] Tatsachendichte“ im „Vorfeldbereich“ hinweist und darüber hinaus argumentiert, dass eine unabhängige Vorabkontrolle nur „ausnahmsweise“ geboten ist, „soweit es um Maßnahmen geht, die sich aufgrund konkreter tatsächlicher Anhaltspunkte gezielt gegen Einzelpersonen richten, um eine Gefahr mit dem Ziel aufzuklären, diese zu unterbinden.“, Gärditz, EuGRZ 2018, 6, 18.

⁴⁴² Möglich sollte das jedoch zumindest bei der Vorabkontrolle der gezielten strategischen Maßnahmen sein (§§ 42 Abs. 1 Nr. 2, 23 Abs. 5, Abs. 7 BNDG), wenn hierfür zukünftig in verfassungskonformer Weise Suchbegriffe in der Anordnung genannt werden müssen (vgl. [Teil 3 C. II. 1. a. bb\) \(2\)](#), [Teil 4 B. I. 3. a. aa\)](#)), denn dann würde wegen der personenbezogenen Suchbegriffe bereits vorher feststehen, gegen wen sich die Maßnahme richtet.

(1) Abmilderung des rechtsstaatlichen Defizits statt Kompensation

In der Überlegung, dass die Rechtskontrolle unbestimmte Eingriffsermächtigungen ausgleichen könne, wird die Tatsache, dass die Rechtskontrolle selbst maßgeblich von der Ausgestaltung der Verhaltensnormen abhängig ist⁴⁴³, nicht ausreichend berücksichtigt. Die Kontrolle kann nicht losgelöst von den Befugnisnormen (auch) als Komponente für deren Rechtfertigung dienen, wenn die Wirksamkeit der Kontrolle ihrerseits maßgeblich von den Befugnisnormen abhängig ist. Zwischen beidem besteht ein untrennbarer Zusammenhang: Die Defizite der Befugnisnormen begründen zugleich ein Defizit bei der Rechtskontrolle.⁴⁴⁴ Ist der Tatbestand der Eingriffsnorm „unbestimmt und darum mangelhaft, so setzt sich der Mangel zwangsläufig in der gerichtlichen Entscheidung fort“.⁴⁴⁵ Für andere unabhängige Vorabkontrollen gilt nichts anderes.

Selbstverständlich kennt auch das Bundesverfassungsgericht diesen Einwand, denn er taucht in einer seiner älteren Entscheidung auf.⁴⁴⁶ Dass es die Ausweitung der Vorabkontrolle dennoch damit begründet, illustriert, wie das Gericht die Rolle des Vorabkontrolleurs eigentlich versteht: der Vorabkontrolleur kontrolliert mehr als „nur“ die Vereinbarkeit mit einfachem Recht und den Grundrechten. Vielmehr wird er dem Nachrichtendienst bei der Anwendung der weiten Rechtsgrundlagen beiseitegestellt und entwickelt im Laufe der Zeit durch sein Fallrecht eine verfassungskonforme Präzisierung des einfachen Rechts.

Auf diese Weise ist nicht nur der Nachrichtendienst für die Handhabbarmachung der (in nachrichtendienstlicher Logik) zwingend weiten Befugnisnormen zuständig. Er kooperiert mit dem Vorabkontrolleur als Korrektiv und neutralem Dritten, der die Wertung des Nachrichtendienstes prüft, indem er das einfache Recht, das mangels Bestimmtheit viele Detailfragen nicht regelt, auslegt und ausdifferenziert. So ist auch die Ausführung des Bundesverfassungsgerichts zu verstehen, wenn es erläutert, die Vorabkontrolle Sorge für die „gebotene verfahrensmäßige Strukturierung der Handhabung“ dieser Befugnisse.⁴⁴⁷ Diese Konzeption der Vorabkontrolle überzeugt: Wenn die Eingriffsnormen schon so weit gefasst sind, dass die handelnde Behörde durch sie kaum beschränkt ist, muss ihre Anwendung wenigstens von einem neutralen Dritten begleitet werden. Schon durch die Begründungspflicht gegenüber dem Vorabkontrolleur und die Kooperation zwischen Kontrolleur und Kontrolliertem entsteht ein rechtsstaatlicher Sicherungsmechanismus.⁴⁴⁸

⁴⁴³ Vgl. [Teil 1 B. III. 4.](#)

⁴⁴⁴ Vgl. [Teil 1 B. III. 4.](#)

⁴⁴⁵ *Bäcker*, Kriminalpräventionsrecht, S. 156.

⁴⁴⁶ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 258.

⁴⁴⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 273.

⁴⁴⁸ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 222.

Bei weiten Befugnissen ist es demnach nicht die Überprüfung der Rechtmäßigkeit anhand eines bereits vorgegebenen normativen Maßstabs, die kompensierend wirkt, sondern die Mitwirkung des neutralen Kontrolleurs bei der notwendigen Handhabarmachung dieser Normen für die Praxis.⁴⁴⁹

Die so verstandene Kontrolle kann das rechtsstaatliche Defizit weiter Eingriffsnormen bei der strategischen Ausland-Fernmeldeaufklärung zumindest abmildern.

(2) Widersprechender Praxisbericht

Auch die Erwartung, dass die Vorabkontrolle der strategischen Ausland-Fernmeldeüberwachung die Weite ihrer Rechtsgrundlagen kompensieren oder zumindest abmildern könnte, enttäuscht Steiner in ihrem Praxisbericht. Sie resümiert, dass die „in den Erhebungsbefugnissen zur verfahrensmäßigen Strukturierung und Eingrenzung der Aufklärungsarbeit verankerten Stellschrauben“ sich wegen der „inhaltlichen Weite und hohen Abstraktion der in den Anordnungen beschriebenen Aufklärungsinteressen“ als „schwer justierbar“ erweisen.⁴⁵⁰

Wenn man dem Bericht von Steiner Glauben schenkt, konnte das GeKon jedenfalls bisher die Erwartung einer Kompensation oder Abmilderung der weiten Befugnisse durch die Vorabkontrolle der strategischen Ausland-Fernmeldeüberwachung und von Eingriffen in informationstechnische Systeme von Ausländern im Ausland nicht erfüllen.

ee) Fokussierung teilweise ungerechtfertigt

Weil die Vorabkontrolle die Erwartungen einer Kompensation der Heimlichkeit und der weiten Befugnisse nicht erfüllen kann, ist die Fokussierung des Bundesverfassungsgerichts auf die Vorabkontrollen nicht nachvollziehbar. Diese Einschätzung kann jedenfalls für Maßnahmen der strategischen Ausland-Fernmeldeaufklärung und Eingriffe in informationstechnische Systeme von Ausländern im Ausland durch den Praxisbericht von Steiner bestätigt werden. Darüber hinaus ist die Leistungsfähigkeit der Vorabkontrolle aber letztlich immer dann in Frage zu stellen, wenn die Betroffenen zum Zeitpunkt der Genehmigung noch nicht bekannt sind oder die Tatbestandsvoraussetzung der Befugnisnorm ähnlich weit formuliert sind wie bei den Normen zur strategischen Ausland-Fernmeldeaufklärung.

⁴⁴⁹ „Viele gesetzliche Bestimmungen zu staatlichen Überwachungstätigkeiten sind relativ unbestimmt und müssen im Einzelfall interpretiert werden. Die gerichtsähnlichen Entscheidungen des UKRats über die Rechtmäßigkeit der technischen Aufklärung nehmen daher eine wichtige Rolle bei der Auslegung und Fortentwicklung des Nachrichtendienstrechts ein.“, *Wetzling*, *Bedingt kontrollfähig*, S. 16.

⁴⁵⁰ *Steiner*, *GSZ* 2023, 124, 130.

b. Vernachlässigung der Datenschutzkontrolle

Die Kehrseite dieser Fokussierung auf die Vorabkontrolle ist, dass das Bundesverfassungsgericht der laufenden bzw. nachträglichen Datenschutzkontrolle in seiner Rechtsprechung zum Nachrichtendienstrecht viel weniger Bedeutung beigemessen hat⁴⁵¹.

aa) Vorteile der laufenden Kontrolle

Das ist mit Blick auf das Ziel der Kompensation fehlender Rechtsschutzmöglichkeiten Betroffener ein Fehler, weil die Informationen, die für die Beurteilung der Rechtmäßigkeit notwendig sind, erst bei der laufenden und nachträglichen Kontrolle definitiv jedenfalls dem Nachrichtendienst, und damit potenziell auch dem Kontrolleur, vorliegen. Mithin kann die Kontrolle zu diesem Zeitpunkt eher kompensierend wirken als die Vorabkontrolle. Steiner bestätigt dies, indem sie ausführt, dass bei der Kontrolle der strategischen Ausland-Fernmeldeaufklärung und von Eingriffen in informationstechnische Systeme von Ausländern im Ausland erst im Laufe der Kontrolle durch das Ad-Kon geprüft werden kann, ob die Datenverarbeitung „für das Aufklärungsanliegen geeignet, erforderlich und verhältnismäßig im engeren Sinne war. Angesichts der verfassungsrechtlichen Vorgaben zur personellen Besetzung des gerichtsähnlichen und des administrativen Kontrollorgans“⁴⁵² liege darin „eine unbefriedigende Schieflage“.⁴⁵³

Den dargelegten Vorteil gegenüber der Vorabkontrolle bietet die Datenschutzkontrolle nicht nur bei der strategischen Überwachung, sondern bei allen nachrichtendienstlichen Maßnahmen, bei denen zum Zeitpunkt der Anordnung noch entscheidende Informationen fehlen, um die Rechtmäßigkeit beurteilen zu können.

bb) Kontrollerggebnisfolgen

Als besonders problematisch erweist sich die Vernachlässigung der Datenschutzkontrolle in Bezug auf die Kontrollerggebnisfolgen. Bisher hat das Bundesverfassungsgericht nur vorgegeben, dass die Befugnisse „wirksam“ sein müssen, weshalb dem Gesetzgeber ein großer Beurteilungsspielraum verbleibt. Die hier vertretene Interpretation des Be-

⁴⁵¹ Vgl. [Teil 2 A. IV. 2. a. aa\).](#)

⁴⁵² Das Bundesverfassungsgericht hat für die Besetzung des gerichtsähnlichen Kontrollorgans höhere Anforderungen formuliert, vgl. [Teil 2 A. III. 1. b. ii\).](#)

⁴⁵³ Steiner, GSZ 2023, 124, 130.

griffs der „Wirksamkeit“, wonach eine Maßnahme nur wirksam ist, wenn ihr beabsichtigter Erfolg eintritt⁴⁵⁴, und aus der folgt, dass den Datenschutzbeauftragten auch gegenüber den Nachrichtendiensten das Recht zur Anordnung verliehen werden muss⁴⁵⁵, teilen Legislative und Exekutive in Bund und Ländern offensichtlich nicht. Stattdessen wird bei Datenschutzverstößen das Beanstandungsrecht als ausreichend erachtet⁴⁵⁶, was praktisch dazu führt, dass die Datenschutzbeauftragten die Beendigung rechtswidriger Datenverarbeitungen nicht erzwingen können.

Wenn das Bundesverfassungsgericht die Kontrolle mit der Kompensation des fehlenden Rechtswegs begründet, diese Kompensation aber in vielen Fällen bei der laufenden Kontrolle besser realisiert werden kann, müsste die laufende Kontrolle ebenso wirksam sein wie die Vorabkontrolle. Dass das Bundesverfassungsgericht die Kontrollergebnisse der Datenschutzkontrollen nicht konkretisiert, bei der Vorabkontrolle hingegen ein verbindliches Entscheidungsrecht vorgibt, überzeugt daher nicht.

cc) Kontrollintervall

Dass die Rechtsprechung des Bundesverfassungsgerichts in Bezug auf die laufenden Kontrollen kritikwürdig ist, lässt sich zudem am Beispiel des Kontrollintervalls veranschaulichen. Nach den Entscheidungen des Bundesverfassungsgerichts muss die Datenschutzaufsicht außerhalb der strategischen Ausland-Fernmeldeaufklärung „regelmäßig“, mindestens aber in einem Abstand von zwei Jahren erfolgen.⁴⁵⁷ Gründe für die Notwendigkeit genau dieses Zeitraums benennt das Bundesverfassungsgericht nicht. Weil es betont hat, dass die Vorabkontrollen nur über die Zulässigkeit einzelner Maßnahmen, nicht aber über die Rechtmäßigkeit ihrer Durchführung entscheiden⁴⁵⁸ und die Rechtmäßigkeit der Datenverarbeitungen (extern) nur die Datenschutzaufsicht kontrolliert, die Kontrolle aber aus mehreren Gründen verfassungsrechtlich erforderlich ist, wären häufigere Kontrollen besser geeignet, den Kontrollzweck zu fördern. Das gilt umso mehr, als der Kontrollzweck einer Kompensation durch die Datenschutzkontrolle besser verwirklicht werden kann.

Dass Kontrollen häufiger erforderlich sein können, erkennt das Bundesverfassungsgericht jedenfalls in Bezug auf die administrative Kontrolle der strategischen Ausland-Fernmeldeaufklärung selbst an.⁴⁵⁹ Wieso für andere eingriffsintensive Maßnahmen der Nachrichtendienste seltenere Kontrollen ausreichen sollen, ist nicht ersichtlich.

⁴⁵⁴ Vgl. [Teil 2 A. III. 1. a. gg\).](#)

⁴⁵⁵ Vgl. [Teil 4 B. I. 4. e. aa\).](#)

⁴⁵⁶ Vgl. [Teil 3 D. II. 6. a.](#)

⁴⁵⁷ Vgl. [Teil 2 A. III. 1. a. ee\).](#)

⁴⁵⁸ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 267; dies trifft auf die G 10-Kommission allerdings nicht zu.

⁴⁵⁹ Vgl. [Teil 2 A. III. 1. b. ee\).](#)

Insgesamt entsteht der Eindruck, das Bundesverfassungsgericht agiere eher pragmatisch und wolle den Gesetzgeber, die Haushalte und die Aufsichtsbehörden mit dieser (willkürlich gewählten) Maximal-Zeitspanne zwischen zwei Kontrollen vor dem Hintergrund unterausgestatteter Datenschutzbehörden⁴⁶⁰ nicht überfordern. Der vom Bundesverfassungsgericht geforderte „Kontroll-Gesamtüberblick“ lässt sich in einer Zeitspanne von bis zu zwei Jahren zwischen zwei Kontrollen jedoch nicht realisieren.

c. Quasi-gesetzgeberische Rolle des Vorabkontrolleurs

Indem das Bundesverfassungsgericht das gerichtsähnliche Kontrollorgan nicht nur als Rechtskontrolleur im eigentlichen Sinne begreift, sondern es dem Nachrichtendienst bei der Handhabarmachung – zum Teil notwendigerweise – weiter Normen beiseite stellt und das gerichtsähnliche Kontrollorgan somit mit der Aufgabe der Rechtsentwicklung betraut, überträgt es ihm eine quasi-gesetzgeberische Funktion.

Wegen dieser Nähe zur Aufgabe des Gesetzgebers wird vertreten, dass die Kompensation weiter Befugnisse am ehesten durch politische Kontrollen verwirklicht werden kann.⁴⁶¹ Andererseits üben die Mitglieder des gerichtsähnlichen Kontrolleurs diese Aufgabe hauptberuflich aus, sind hoch spezialisiert und können daher umfassender kontrollieren als es Parlamentariern, die viele weitere Aufgaben übernehmen, möglich wäre. Hinzu kommt, dass die Rechtsentwicklung häufig nicht nur durch das Parlament, sondern auch durch Gerichte erfolgt. Ein eindruckliches Beispiel dafür ist die Rechtsprechung des Bundesverfassungsgerichts zum Nachrichtendienstrecht. Dass das Bundesverfassungsgericht dem gerichtsähnlichen Kontrollleur – und nicht etwa dem parlamentarischen Kontrollgremium – eine quasi-gesetzgeberische Funktion überträgt, ist daher schlüssig.

⁴⁶⁰ Schütz, Zum Leben zu wenig, zum Sterben zu viel?, 251, 265 ff.; Kutscha, NVwZ 2003, 1296, 1299.

⁴⁶¹ So äußerte sich Borgs-Maciejewski bereits 1977, als es außer dem G 10 keine Rechtsgrundlagen gab: „Wenn aus den Sachzwängen, denen die Dienste unterliegen, folgt, daß eine exakte Eingriffsermächtigung in hohem Maße schädlich wäre, so müßte die mangelnde Bestimmtheit durch ein Mehr an parlamentarischer Kontrolle ausgeglichen werden“ sowie „Die beschränkten Möglichkeiten des Parlaments zur Normsetzung im Bereich der Geheimdienste lassen die Forderung einleuchtend und konsequent erscheinen, das Parlament hier wenigstens so weit wie möglich Einfluß nehmen zu lassen. Wenn das Parlament seine staatsleitende Funktion nicht in vollem Umfang mit den Mitteln der Gesetzgebung verwirklichen kann, wird seine Prärogative am ehesten durch Kontrolle gewahrt.“, Borgs-Maciejewski, Unzulängliche Kontrolle; Friesenbahn, Kontrolle, 87, 99 erachtet dies jedenfalls bei „auf Ausländer im Ausland bezogenen“ Sachverhalten des BND als sinnvoll, weil insoweit über die „außen- und sicherheitspolitische Zweckmäßigkeit“ zu entscheiden sei, die „eher von einem politischen Gremium zu bewerten“ sei, insoweit fordert er eine „echte politische Präventivkontrolle“, Bartodziej, Hdb. des Rechts der Nachrichtendienste, 1533, 1605 f.

Aus dieser quasi-gesetzgeberischen Funktion folgt allerdings, dass das Parlament den gerichtsähnlichen Kontrollleur legitimieren muss.⁴⁶² Deshalb ist es richtig und wichtig, dass dessen Mitglieder nach geltendem Recht vom parlamentarischen Kontrollgremium gewählt werden⁴⁶³ und ihm regelmäßig Bericht erstatten müssen⁴⁶⁴.

d. Schaffung eines (zu) mächtigen Akteurs?

Weil das gerichtsähnliche Kontrollorgan mit der Handhabbarmachung weiter Normen auch gesetzgebungsähnliche Funktionen wahrnimmt, ist es ein sehr mächtiger Akteur.

Es ist überzeugend, die Konkretisierung weiter Normen nicht allein der Behörde zu überlassen und sie zur Kooperation mit einem unabhängigen Kontrollleur zu verpflichten, wenn man wie das Bundesverfassungsgericht die Notwendigkeit weiter Befugnisse jedenfalls für bestimmte Bereiche grundsätzlich anerkennt. Nicht nachvollziehbar ist aber, dass das Bundesverfassungsgericht keinerlei Vorkehrungen gegen einen potenziellen Machtmissbrauch des einflussreichen Vorabkontrollleurs trifft.

So wäre es vorstellbar, dass eine dem nachrichtendienstlichen Anliegen (über ein normales Maß hinaus) gewogene Mehrheit im gerichtsähnlichen Kontrollorgan weit mehr Anordnungen genehmigt als es nach gründlicher Würdigung der Betroffeneninteressen eigentlich vertretbar ist. Dass diese Überlegung nicht abwegig ist, zeigt der erste Bericht des UKRats an das PKGr, der an die Presse leaked worden ist. Demnach habe das GeKon „nahezu jede vom BND beantragte Überwachungsmaßnahme“ genehmigt.⁴⁶⁵

Die umgekehrte Situation, in der das Kontrollorgan dem kontrollierten Nachrichtendienst ungerechtfertigt kritisch gegenübersteht, ist ebenso denkbar.

Darüber hinaus gab es zwischen den Mitgliedern des GeKons Streitigkeiten über die Ausgestaltung der Kontrolltätigkeit, die ein so großes Ausmaß erreicht haben, dass zwei Mitglieder des GeKon zum 1. April 2024 zurückgetreten sind.⁴⁶⁶

aa) Minderheitenrechte

Vor diesem Hintergrund weist *Fabrner* zu Recht darauf hin, dass der Diskurs in einem derart mächtigen Gremium zwingend pluralistisch ausgestaltet werden muss, um eine

⁴⁶² “If the problem for parliamentary accountability bodies can be summarized in the word ‘competence’, the problem for expert bodies can be summarized in the word ‘legitimacy’ (...) Moreover, in order to maintain parliament’s confidence in the expert body it is necessary to provide for institutional links between the two.“, *Venedig-Kommission*, Report 2015, S. 51 Rn. 231.

⁴⁶³ § 43 Abs. 1, 4, § 45 Abs. 2 BNDG, [Teil 3 C. IV. 1. a.](#)

⁴⁶⁴ § 55 Abs. 1, 3 BNDG, [Teil 3 C. IX. 3.](#)

⁴⁶⁵ *Bewarder/Flade*, Lauschangriff.

⁴⁶⁶ *Bewarder/Flade*, Machtkampf.

„effektive Auseinandersetzung mit“ und eine „Berücksichtigung“ von „abweichende[n] Ansichten“ sicherzustellen, weshalb Minderheitenrechte von zentraler Bedeutung sind.⁴⁶⁷ Allerdings kann die Notwendigkeit von Minderheitenrechten nicht aus der Gerichtsähnlichkeit der Kontrolle hergeleitet werden.⁴⁶⁸ Stattdessen ergibt sie sich daraus, dass ein zwingend unabhängiger, aber mächtiger Kontrolleur im Rechtsstaat seinerseits der Kontrolle bedarf. Eine gegenseitige Kontrolle der einzelnen Mitglieder innerhalb des GeKons, die durch effektive Minderheitenrechte ermöglicht wird, könnte hierzu einen entscheidenden Beitrag leisten. Dass das Bundesverfassungsgericht festhält, dass den Kontrollinstanzen „die Festlegung ihres Verfahrens und die Wahl ihrer Methoden selbst zu überantworten“ ist, „soweit diese nicht gesetzlich festgelegt sind“⁴⁶⁹, aber keine Überlegungen für eine (Binnen-)Kontrolle des Gremiums äußert, überzeugt daher nicht.

bb) Veröffentlichung von Entscheidungsgründen

Eine weitere Möglichkeit, etwaigen Missbrauch zu verhindern, besteht darin, das GeKon (unter Wahrung der Geheimhaltungsvorschriften) zur Veröffentlichung von Entscheidungsgründen zu verpflichten.⁴⁷⁰ Auf diese Weise wäre es der Öffentlichkeit und der Wissenschaft möglich, die Auslegung der weiten Normen zu beeinflussen.

cc) Rechtfertigungsdruck gegenüber dem Parlamentarischen Kontrollgremium

Gärditz weist zu Recht darauf hin, dass eine Kontrolle des UKRats durch das PKGr problematisch ist, weil das Kontrollmodell des Bundesverfassungsgerichts auf einer Trennung der parlamentarischen von der rechtlichen Nachrichtendienstkontrolle basiert.⁴⁷¹ Andererseits darf das mächtige GeKon bei der gesetzgebungsähnlichen Ausgestaltung der weiten Normen auch nicht kontrollfrei gestellt sein. Eine weitere Möglichkeit, hier Abhilfe zu schaffen, sind Kontrollmöglichkeiten des Parlamentarischen Kontrollgremiums, die aber mit Augenmaß erfolgen müssen: Beispielsweise ist es sinnvoll, dass die Mitglieder des GeKon vom PKGr gewählt werden und der UKRat ihnen gegenüber Bericht erstattet⁴⁷².

⁴⁶⁷ *Fabrner*, GSZ 2023, 223, 227.

⁴⁶⁸ Vgl. [Teil 2 A. III. 6. b. aa](#)).

⁴⁶⁹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 290.

⁴⁷⁰ Vgl. [Teil 4 I. 3. f. aa](#)) (2).

⁴⁷¹ Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 14 f.

⁴⁷² Vgl. [Teil 3 C. IV. 1. a](#), [Teil 3 C. IX. 3](#).

Die Kontrolle des UKRat durch den BfDI kann diese Aufgabe nicht erfüllen, weil der BfDI selbst ein Organ der Exekutive ist, das etwaigen Missbrauch bei der gesetzgebungsähnlichen Funktion des GeKons nicht verhindern kann.

dd) Fazit

Dass das Bundesverfassungsgericht in seiner detaillierten Rechtsprechung zur Rechtskontrolle der Nachrichtendienste keinen dieser Aspekte angesprochen hat, ist nicht nachvollziehbar.

e. Nebeneinander von Kontrollstrukturen

Die sich zum Teil überschneidenden Kontrollstrukturen und der daraus folgende Mehraufwand für die Nachrichtendienste werden seit Jahren diskutiert und zu Recht kritisiert.⁴⁷³ Trotzdem hat dieses Problem in der Rechtsprechung des Bundesverfassungsgerichts bisher keine Berücksichtigung gefunden.⁴⁷⁴

Teilweise hat das Bundesverfassungsgericht die Schaffung neuer Strukturen sogar befördert. Als es in seiner Entscheidung zur strategischen Ausland-Fernmeldeaufklärung 2020 ein administratives Kontrollorgan forderte, hat es sich – wohl aus Rücksicht auf den Regelungsspielraum des Gesetzgebers – nicht auf den BfDI festgelegt⁴⁷⁵, obwohl der BfDI für die Datenschutzkontrolle anderer nachrichtendienstlicher Maßnahmen zuständig ist. An dieser Stelle hätte es mit Verweis auf die Verhinderung der Etablierung eines zusätzlichen Kontrolleurs einen guten Grund gegeben, den Regelungsspielraum des Gesetzgebers zu verengen und sich in der Entscheidung auf den BfDI als administrativen Kontrolleur festzulegen.⁴⁷⁶ Bei der Reform zur Umsetzung der Entscheidung hat sich der Gesetzgeber dann dafür entschieden, mit dem AdKon einen weiteren Kontrolleur zu schaffen.

Darüber hinaus hat das Bundesverfassungsgericht über die beschränkte Kontrollzuständigkeit der G 10-Kommission und die Abgrenzung der Zuständigkeit von G 10-

⁴⁷³ Vgl. [Teil 4 A. I.](#)

⁴⁷⁴ Die Problematik wird nur am Rande gestreift: In BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 216 fordert das Bundesverfassungsgericht die Kooperation der Datenschutzbeauftragten von Bund und Ländern, in BVerfG BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290 stellt es klar, dass die kontrollierende Stelle alle Maßnahmen, denen eine Person durch eine Behörde ausgesetzt ist, in den Blick nehmen können muss, was sich so interpretieren lässt, dass Kenntnisbeschränkungen einzelner Kontrolleure (zugunsten anderer Kontrolleure) zu vermeiden sind, in BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 297 fordert es einen engen Austausch zwischen dem gerichtsähnlichen und dem administrativen Kontrolleur.

⁴⁷⁵ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 282; *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 581.

⁴⁷⁶ So auch *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 532.

Kommission und BfDI bis heute nicht entschieden, obwohl ihm seit 2016 eine Verfassungsbeschwerde vorliegt, in der dieses Problem adressiert wird.⁴⁷⁷

Hinzu kommt das Nebeneinander von G 10-Kommission und UKRat, das das Bundesverfassungsgericht hätte adressieren können, aber nicht adressiert hat. Aus der Entscheidung zur strategischen Ausland-Fernmeldeaufklärung wird deutlich, dass die Vorabkontrolle dieser Maßnahmen nicht der G 10-Kommission übertragen werden sollte. Die dadurch entstehende Aufspaltung der Vorabkontrolle von strategischen Maßnahmen, die Deutsche und Inländer betreffen und solchen, die nur Ausländer im Ausland betreffen, problematisiert das Bundesverfassungsgericht aber nicht. Letztlich spiegeln sich in dieser Rechtsprechung die Konstruktionsprobleme des einfachen Rechts: die Regelung bestimmter Befugnisse der Nachrichtendienste im G 10 statt in den jeweiligen Fachgesetzen ist längst überholt, deshalb besteht in der Wissenschaft weitgehend Konsens, dass die G 10-Befugnisse in die Fachgesetze integriert werden müssen⁴⁷⁸. Dass das Bundesverfassungsgericht dieses Problem nicht lösen kann, wenn es über eine Verfassungsbeschwerde zum BNDG zu entscheiden hat, ist logisch. Es hätte aber die Gelegenheit gehabt, dem Gesetzgeber im Rahmen der Ausführungen zu einem neuen Kontrollorgan einen Prüfauftrag zu erteilen, inwieweit die Tätigkeit der G 10-Kommission integriert werden könnte.⁴⁷⁹

Es ist nicht nachvollziehbar, dass das Bundesverfassungsgericht Anreize schafft, neue Kontrollstrukturen aufzubauen, ohne zugleich einer weiteren Erhöhung der ohnehin problematisch hohen Anzahl der Rechtskontrolleure vorzubeugen.

f. Zu detaillierte Ableitung aus der Verhältnismäßigkeit

Eine häufig geäußerte Kritik betrifft die Herleitung von Kontrollanforderungen aus dem Verhältnismäßigkeitsprinzip. Mehrere Sondervoten zu Bundesverfassungsentscheidungen wurden unter anderem damit begründet, dass der Gestaltungsspielraum

⁴⁷⁷ Bäckers, Beschwerdeschrift G 10, S. 64 ff.

⁴⁷⁸ Aust, DöV 2020, 715, 723; Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 16; Dietrich, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 24; mit konkreten Vorschlägen Vogt, Strategische Auslandstelekommunikationsüberwachung, S. 646 ff.; zu den praktischen Problemen Steiner, GSZ 2023, 124, 127.

⁴⁷⁹ Einen solchen Prüfauftrag hat es beispielsweise zur Anrufungsmöglichkeit von Betroffenen formuliert, vgl. BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 280.

des Gesetzgebers durch die aus der Verhältnismäßigkeitsprüfung entwickelten Vorgaben zu weitgehend eingeschränkt würde.⁴⁸⁰ Ein dissentierender Richter schreibt im Urteil zum Bundeskriminalamtsgesetz:

„Der Senat setzt mit zahlreichen gesetzgebungstechnischen Detailanforderungen letztlich seine konkretisierenden eigenen Vorstellungen von dem Regelwerk in meines Erachtens zu weit gehender Weise an die Stelle derjenigen des demokratisch legitimierten Gesetzgebers, der sich für seine Konzeption politisch zu verantworten hat und diese gegebenenfalls auch leicht korrigieren kann.“⁴⁸¹

Ein Beispiel für eine detaillierte Ausgestaltung, die ein dissentierende Richter ablehnt, ist die Festlegung auf ein Mindestkontrollintervall von zwei Jahren bei der Datenschutzaufsicht.⁴⁸² Auch aus der Wissenschaft werden Forderungen nach mehr richterlicher Zurückhaltung geäußert. Zu den im Urteil zur strategischen Auslands-Fernmeldeaufklärung⁴⁸³ etablierten Anforderungen an die richterähnliche Kontrolle der Fernmeldeüberwachung schrieb Gärditz beispielsweise:

„Es fällt schwer, solche Details – mögen sie auch rechtspolitisch klug sein – als Konsequenz der Verhältnismäßigkeit auszuflaggen. Pflichtschuldige Hinweise auf die Gestaltungsspielräume des Gesetzgebers nehmen daneben beinahe satirischen Charakter an.“⁴⁸⁴

Insbesondere die Herleitung des richterähnlichen Kontrollniveaus aus der Verhältnismäßigkeit wurde wiederholt angegriffen, denn neben den ausdrücklichen, geschriebenen Richtervorbehalten (beispielsweise in Art.13 Abs. 2 – 4 GG) sei für ungeschriebene Richtervorbehalte kein Raum.⁴⁸⁵ Die Vorgehensweise des Bundesverfassungsge-

⁴⁸⁰ BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 - 1. Sondervotum Rn. 326, Anforderungen nach Art einer „Handlungsanleitung“; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 Sondervotum 1 Rn. 5, Sondervotum 2 Rn. 2 ff.

⁴⁸¹ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - 2. Sondervotum Rn. 2.

⁴⁸² BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - 1. Sondervotum Rn. 7.

⁴⁸³ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17.

⁴⁸⁴ Gärditz, JZ 2020, 825, 833.

⁴⁸⁵ Gärditz, JZ 2020, 825, 833; „Auf diese Weise wird das ungeschriebene Verfassungsrecht (Verhältnismäßigkeitsgrundsatz) über das geschriebene Verfassungsrecht gesetzt, was grundsätzlich nicht zulässig ist“, Wolff, NVwZ 2010, 751, 752; Durner, DVBl 2016, 780, 782; Lindner/Unterreitmeier, DöV 2019, 165, 174.

richts bewirke die „Einebnung der Differenzierungen des geschriebenen Verfassungsrechts“ und führe zu einem „Bedeutungsverlust des Verfassungswortlauts“. ⁴⁸⁶ Die kritischen Anmerkungen wurzeln im Gewaltenteilungsprinzip, das die Kritiker verletzt sehen. ⁴⁸⁷

Diesem Befund ist grundsätzlich zuzustimmen. Wenn das Verfassungsgericht die gestalterischen Anforderungen auf der Ebene der Verhältnismäßigkeitsprüfung ausdifferenziert, wirkt sich dies zugleich verengend auf den Gestaltungsspielraum des Gesetzgebers aus. ⁴⁸⁸ In Anbetracht der Tatsache, dass es grundsätzlich die Aufgabe der Legislative ist, Normen zu gestalten, das Bundesverfassungsgericht hier aber ebenfalls gestaltend tätig wird, klingen die Forderungen nach stärkerer richterlicher Zurückhaltung zur Austarierung der Gewalten plausibel.

Aber was folgt daraus? Erstens ist unklar, wann ein „zu viel“ der aus der Verhältnismäßigkeit im engeren Sinne abgeleiteten Vorgaben erreicht ist, dass die Verhältnismäßigkeitsvorgaben problematisch werden lässt. Wichtiger ist jedoch zweitens die Frage danach, welche Optionen dem Bundesverfassungsgericht praktisch verblieben, wollte es die Forderungen umsetzen. Schließlich ist es nicht sein gestalterischer Wille, der es dazu treibt, diese Vorgaben zu formulieren, sondern eine verfassungsrechtliche Notwendigkeit. Bezogen auf die aus der Verhältnismäßigkeit abgeleiteten Vorgaben an die Kontrolle der Sicherheitsbehörden ist festzuhalten, dass die Kontrolle selbst ein Gebot des Rechtsstaatsprinzips ist und der Wegfall des subjektiven Rechtsschutzes im Nachrichtendienstrecht wegen Art. 19 Abs. 4 GG effektiv kompensiert werden muss. ⁴⁸⁹

Würde das Bundesverfassungsgericht die Kritik umsetzen wollen, hätte es die Möglichkeit, die Befugnisnorm so oft als verfassungswidrig zu beurteilen, bis der Gesetzgeber von sich aus ein ausreichend effektives Kontrollniveau geschaffen hat. Ob bei einer in diesem Sinne verstandenen richterlichen Zurückhaltung mehr Spielraum für den Gesetzgeber geschaffen würde, ist fraglich. ⁴⁹⁰ Grundrechtsschonender ist sie nicht.

⁴⁸⁶ Durner, DVBl 2016, 780, 782.

⁴⁸⁷ So explizit ebd.; Graulich, GSZ 2021, 121, 122; Alt, Kompensatorische Kontrolle, S. 243, 270.

⁴⁸⁸ Barczak, KritV 2021, 91, 100, 101.

⁴⁸⁹ Vgl. [Teil 2 A. I. 2.](#)

⁴⁹⁰ Vor allem wäre dies einer Systematisierung abträglich, außerhalb der jeweils entschiedenen Fallkonstellation würde dies erhebliche Rechtsunsicherheiten verursachen, so Bäcker, Hdb. des Verfassungsrechts, 1715, 1776 Rn. 187.

g. Richtervorbehalt als effektivstes Mittel?

Das Bundesverfassungsgericht hat in mehreren Urteilen verdeutlicht, dass es die richterliche Kontrolle gegenüber anderen unabhängigen Kontrollinstitutionen bevorzugt⁴⁹¹, weil die sachliche und persönliche Unabhängigkeit der Richter sowie ihre ausschließliche Bindung an das Gesetz die Betroffenenrechte am sichersten zu schützen vermöge.⁴⁹² Seine Präferenz für die gerichtliche Kontrolle offenbart sich zudem darin, dass diese häufig der Referenzpunkt für Anforderungen ist, beispielsweise, wenn eine andere unabhängige Kontrollinstitution „die gleiche Gewähr für die Unabhängigkeit und Neutralität“ bieten müsse „wie ein Richter“.⁴⁹³ Demgegenüber wird in der Literatur an der Vorabkontrolle durch Richter Kritik geübt.

aa) Institutionelle Neutralität

Das Bundesverfassungsgericht sieht den Vorteil der richterlichen Vorabkontrolle vor allem in der institutionell abgesicherten Unabhängigkeit der Gerichte.

Soweit eine andere Kontrollinstitution unabhängig und weisungsfrei ausgestaltet wird, ist eine vergleichbare sachliche Unabhängigkeit garantiert, wie sie für Richter gem. Art. 97 Abs. 1 GG vorgesehen ist. Anders als beispielsweise die ehrenamtlich tätigen Mitglieder der G 10-Kommissionen, die lediglich eine Aufwandsentschädigung erhalten, sind die Richter wegen ihrer angemessenen Besoldung darüber hinaus persönlich unabhängig gem. Art. 97 Abs. 2 GG.⁴⁹⁴

Dieser Aspekt spricht dafür, die richterliche Kontrolle als „neutraler“ einzustufen. Allerdings ist es möglich, auch bei einer anderen Kontrollinstitution eine angemessene Besoldung vorzusehen, die deren Mitglieder eine vergleichbare persönliche Unabhängigkeit vermitteln könnte.

bb) Fehlende Sensibilität für Grundrechtsschutz durch Verfahren

Ein häufig vorgebrachter Einwand gegen Richtervorbehalte im Sicherheitsrecht betrifft die Frage, wie engagiert die Richter den Fall tatsächlich überprüfen. Eine empirische Studie⁴⁹⁵, in der die Anordnungspraxis von vier Staatsanwaltschaften bei der Telefon-

⁴⁹¹ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259, 260; BVerfG, Urteil v. 2.3.2010 - 1 BvR 256/08 Rn. 248.

⁴⁹² BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259, 260.

⁴⁹³ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 - 1 BvR 595/07 - Rn. 259, 260; oder dahingehend, dass die unabhängige Kontrolle „gleichwertig“ zur gerichtlichen Kontrolle sein muss, BVerfG, Urteil v. 15.12.1970 - 2 BvF 1/69 - 2 BvR 629/68 - 2 BvR 308/69 Rn. 77.

⁴⁹⁴ Bantlin, G 10-Kommission, S. 155.

⁴⁹⁵ Backes/Gusy, Wer kontrolliert die Telefonüberwachung?.

überwachung untersucht wurde, kam zu ernüchternden Ergebnissen: Bei 307 Anträgen auf Überwachung haben die Richter nur einen Antrag abgelehnt und mehr als 90 % der staatsanwaltlichen Antragstexte wörtlich übernommen. Die im Rahmen der Untersuchung interviewten Richter und Staatsanwälte würden die Interessen der Betroffenen nicht berücksichtigen und empfänden ihre Kontrolle nicht als „eine besondere Form des Grundrechtsschutzes“. Ihnen würde jegliche Sensibilität dafür fehlen, dass es sich bei den genehmigten Maßnahmen um Grundrechtseingriffe handelt.⁴⁹⁶

Die Ergebnisse der Studie sind aus heutiger Sicht jedoch nicht sehr aussagekräftig, da die Studie mittlerweile über zwanzig Jahre alt ist und die Begründungsanforderungen damals weitaus geringer waren. Ob und inwieweit dies bei der richterlichen Überprüfung nachrichtendienstlicher Befugnisse ähnlich gehandhabt wird, ist empirisch noch nicht untersucht. Die Gründe, die die fehlende Sensibilität der Richter (mit-)verursachen können, sind allerdings auf die für die Nachrichtendienste zuständigen Kontrolleure übertragbar: Als Ursache wird beispielsweise die enorme Arbeitsbelastung genannt⁴⁹⁷.

cc) Umfang

Im Kontext einer möglichen Ausweitung des Richtervorbehalts wird angemerkt, dass damit eine erhebliche Mehrbelastung der Gerichte einhergehe. Dass jede einzelne eingriffsintensive Maßnahme der Nachrichtendienste genehmigt werden müsse und es sich bei diesen Maßnahmen um das „Kerngeschäft der Dienste“ handle, verdeutliche den Umfang der Mehrarbeit, die durch eine Erweiterung des Richtervorbehalts entstehe. In diesem Fall müsste an allen Nachrichtendienststandorten nicht nur die Anzahl der Richterstellen, sondern auch die der Urkundsbeamten und Geschäftsstellenmitarbeiter erhöht werden.⁴⁹⁸

Das Bundesverfassungsgericht ist sich dieses Problems bewusst. Im Urteil zum Bundeskriminalamtsgesetz verpflichtet der Senat die Justizverwaltung zur Lösung: „Hierfür [Anm.: für die richterliche Kontrolle] die notwendigen sachlichen und personellen Voraussetzungen zu schaffen, obliegt der Landesjustizverwaltung und dem Präsidium des zuständigen Gerichts.“⁴⁹⁹

Im Vergleich zu den G 10-Kommissionen stellt man fest, dass der deutschen Gerichtsbarkeit wesentlich mehr Richter zur Verfügung stehen als die jeweiligen G 10-

⁴⁹⁶ *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, S. 128; *Kutscha*, NVwZ 2003, 1296, 1298 f.; *Bäcker*, Kriminalpräventionsrecht, S. 158, der in Fn. 319 auf weitere Studien verweist.

⁴⁹⁷ *Bäcker*, Kriminalpräventionsrecht, S. 158.

⁴⁹⁸ *Weisser*, DöV 2014, 831, 835.

⁴⁹⁹ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 118.

Kommissionen Mitglieder haben.⁵⁰⁰ Daher verwundert es nicht, dass die geringe Mitgliederzahl der G 10-Kommissionen ebenfalls kritisiert wird.

Die Kritik an der geringen Anzahl der Mitglieder der G 10-Kommission verdeutlicht, dass es sich nicht um ein originäres Problem der Verwaltungsrechtsprechung handelt, sondern dass eine ausreichende Personalausstattung bei der Vorabkontrolle institutionsübergreifend von zentraler Bedeutung ist.⁵⁰¹

dd) Geheimhaltungsbedenken

Einige kritisieren die Einbindung der Richter, weil sie befürchten, dadurch könnten geheimhaltungsbedürftige Informationen kompromittiert werden.⁵⁰²

Die Gefahr besteht insbesondere, wenn die mit der Entscheidung befassten Gerichte schlecht abgeschirmt sind. Möglich wäre, dass andere, feindlich gesinnte Staaten den Kontrollmoment ausnutzen, weil sie so vergleichsweise leicht an Informationen gelangen können. Um dies zu verhindern, wird zu Recht gefordert, dass die Räumlichkeiten abgesichert und alle Mitarbeiter und Mitarbeiterinnen überprüft werden müssen.⁵⁰³

Das Bundesverfassungsgericht selbst spricht diese Bedenken in seinem Urteil zum Bayerischen Verfassungsschutzgesetz an und verweist darauf, dass die Vorabkontrolle durch ein Gericht „nicht grundsätzlich vorgegeben sei“ und es für den Gesetzgeber „nicht unmöglich“ wäre, die Geheimhaltung wahrende, unabhängige Stellen zu schaffen.⁵⁰⁴ Im Ergebnis kommt es bezüglich der Geheimhaltungsbedenken nicht entscheidend darauf an, wer der Kontrolleur ist. Wichtiger ist, dass die kontrollierende Instanz ausreichend gegen Spionage geschützt ist. Dass dies grundsätzlich möglich ist, verdeutlicht die Tatsache, dass Geheimhaltungsbedenken bei den Nachrichtendiensten nicht als Argument gegen ihre Existenz angeführt werden, sondern als Hindernis betrachtet werden, das aus dem Weg geräumt wird. Vor dem Hintergrund begrenzter Haushaltsmittel⁵⁰⁵ ist es sinnvoll, nicht die Vielzahl der potenziell mit nachrichtendienstlichen Maßnahmen befassten Gerichte absichern zu müssen, sondern stattdessen wenige oder sogar nur eine spezialisierte Vorabkontrollinstitution(en) zu etablieren.

⁵⁰⁰ Bantlin, G 10-Kommission, S. 158 f.

⁵⁰¹ Z.B. das Bundesverfassungsgericht zur unabhängigen Kontrolle im Anwendungsbereich von Art. 10 Abs. 2 S. 2 GG in BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 304.

⁵⁰² Gefährdung durch „Verbreitung des operativen Wissens“ bei Gärditz, EuGRZ 2018, 6, 17 f.; Weisser, DöV 2014, 831, 835.

⁵⁰³ Weisser, DöV 2014, 831, 835, der jedoch darauf hinweist, dass diese Forderung „vor dem Hintergrund der knappen Landeshaushaltsmittel“ „nicht praktikabel“ sei.

⁵⁰⁴ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 224, hier verweisen die Richter auf § 15 Abs. 2 G 10, der die Geheimhaltungsvorkehrungen bei der G 10-Kommission festlegt.

⁵⁰⁵ Weisser, DöV 2014, 831, 835.

ee) Vorwurf der mangelnden Kompetenz

Teilweise wird als Kritik gegenüber dem Richtervorbehalt im Nachrichtendienstrecht vorgebracht, dass die Kontrolle eine „konkrete wie abstrakte nachrichtendienstliche Expertise“ voraussetze. Anders als beispielsweise in der Strafverfolgung oder der Gefahrenabwehr sei die Bewertung nachrichtendienstlicher Maßnahmen „stärker abhängig von Erfahrung, Fachwissen und – konkret – nachrichtendienstlichen Erkenntnislagen“. Diese Fähigkeiten könnten externe Institutionen wie Gerichte nicht „angemessen“ ersetzen oder sich aneignen.⁵⁰⁶

Die bayerische Landesregierung schloss sich im Verfahren zum Bayerischen Verfassungsschutzgesetz dieser Argumentation an: Mangels „überschaubarer Erkenntnislage“, die „nach Aktenlage“ beurteilt werden könne, sei eine richterliche Vorabkontrolle nicht möglich.⁵⁰⁷

Das Bundesverfassungsgericht stimmt dem insoweit zu, dass die externe Stelle „nicht ohne Weiteres“ über eine vergleichbare Expertise verfüge wie die Mitarbeiter und Mitarbeiterinnen der Nachrichtendienste. Die Verfassungsschutzbehörde müsse jedoch in der Lage sein, ihr „Wissen und die daraus abgeleitete Interpretation der Verdachtssituation in einer Weise darzulegen, dass deren Plausibilität zumindest nachvollziehend geprüft werden kann.“ Die Behörde müsse sich selbst und den unabhängigen Kontrolleuren „Rechenschaft ablegen können“, ob die Anhaltspunkte für den verfassungsschutzspezifischen Beobachtungsbedarf tatsächlich vorliegen. Wenn ihr dies nicht möglich sei, betont das Gericht, könne „die verfassungsrechtlich erforderliche Eingriffsschwelle kaum erreicht sein“.⁵⁰⁸

Das Bundesverfassungsgericht entgegnet dem vorgebrachten Argument damit, dass die Verantwortung dafür, ob das Vorliegen der Eingriffsvoraussetzungen geprüft werden kann, bei den Verfassungsschutzbehörden liegt, weil diese verpflichtet sind, ihre Anträge nachvollziehbar zu begründen.⁵⁰⁹ Auf das Vorhandensein von Fachwissen beim Kontrolleur soll es insoweit nicht entscheidend ankommen.

Darüber hinaus ist die Expertise der Nachrichtendienste für die Mitglieder externer Kontrollinstitutionen erlernbar. Soweit entgegnet wird, dass ein Kontrolleur zuerst

⁵⁰⁶ Gärditz, EuGRZ 2018, 6, 18; entsprechend Lindner/Unterreitmeier, DöV 2019, 165, 174.

⁵⁰⁷ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 73.

⁵⁰⁸ Ebd. Rn. 221, darüber hinaus weist das Gericht darauf hin, dass die Verfassungsschutzgesetze Normen enthalten, die eine Begründung gegenüber dem zuständigen Innenministerium vorschreiben. Wenn dies möglich sei, könne es gegenüber einer externen Stelle nicht unmöglich sein.

⁵⁰⁹ Das Gericht argumentiert mit der „Ordnungsfunktion“ von Kontrollen, die nach Bäcker die „Zäsur-, Strukturierungs- und Fokussierungswirkung der Eingriffsermächtigung“ verstärkt, Bäcker, Kriminalpräventionsrecht, S. 156 f.

„eine Lehre beim Verfassungsschutz“ machen müsste⁵¹⁰, um über vergleichbares Fachwissen zu verfügen, muss die Frage erlaubt sein, warum das so abwegig sein soll. Theoretisch wäre es jedenfalls möglich, die Verantwortlichen der Kontrollinstitution so auszubilden, dass sie die Entscheidungen der Nachrichtendienste nicht nur auf Plausibilität, sondern umfassend prüfen können. Letztlich geht es eher um die Frage, ob die politischen Entscheidungsträger willens sind, diesen Aufwand zu betreiben als darum, dass Externe per se nicht in der Lage wären, sich vergleichbares Fachwissen zu erarbeiten.

ff) Zwischenergebnis

Bei den meisten diskutierten Kritikpunkten bleibt festzuhalten, dass es sich nicht um Probleme handelt, die sich nur bei der Vorabkontrolle durch ein Gericht stellen. Ob die Kontrolleure kompetent genug und sich ihrer Verantwortung hinreichend bewusst sind sowie ausreichend ausgestattet werden, um die Vielzahl der Anträge bearbeiten zu können, sind Fragen, die sich unabhängig davon stellen, welche Institution der Gesetzgeber etabliert hat. Hinsichtlich der Sicherheitsmaßnahmen zum Geheimnisschutz muss festgehalten werden, dass eine einzelne Kontrollinstitution im Vergleich zur Vielzahl potenziell damit befasster Gerichte (ein Gericht am Hauptsitz des jeweiligen Nachrichtendienstes, also mindestens 17) effizienter abgesichert werden kann. Im Ergebnis sind keine Gründe ersichtlich, wieso die Vorabkontrolle durch Richter der Kontrolle durch eine andere unabhängige Institution vorzuziehen sein sollte. Für die Frage, welches Kontrolldesign verfassungsrechtlich vorgegeben ist, ist dies ohnehin wenig relevant, seitdem das Bundesverfassungsgericht eine der richterlichen Vorabkontrolle vergleichbar neutrale Institution als äquivalent anerkannt hat.

B. Völkerrechtliche und unionsrechtliche Vorgaben an die Kontrollnormen

Nachdem auf der Suche nach Maßstäben für die externe Nachrichtendienstkontrolle der Blick zuerst auf das deutsche Verfassungsrecht gerichtet wurde (Teil 2 A.), sollen im Folgenden das Völkerrecht (Teil 2 B. I.) sowie das Recht der Europäischen Union (Teil 2 B. II.) hinsichtlich etwaiger Vorgaben für die Rechtskontrolle der Nachrichtendienste analysiert werden.

⁵¹⁰ So der Bevollmächtigte der bayerischen Landesregierung in der Mündlichen Verhandlung zur Verfassungsbeschwerde gegen das Bayerische Verfassungsschutzgesetz am 14. Dezember 2021.

I. Völkerrechtliche Maßgaben: die Europäische Menschenrechtskonvention

„Freiheitsschutz ist eine Gewährleistungsaufgabe des Staates, des Nationalstaates, der EU, aber auch der gesamten Völkergemeinschaft.“

Prof. Dr. Wolfgang Hoffmann-Riem⁵¹¹

Auf völkerrechtlicher Ebene sind die Vorgaben der Europäischen Menschenrechtskonvention in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte von zentraler Bedeutung.⁵¹²

Die EMRK ist ein die Unterzeichnerstaaten bindender, völkerrechtlicher Vertrag.⁵¹³

1. Innerstaatliche Wirkung

In der Bundesrepublik hat die EMRK den Rang eines verbindlichen Bundesgesetzes.⁵¹⁴ Außerdem wirkt sie im Verfassungsrecht interpretationsleitend und muss bei der Auslegung der Grundrechte berücksichtigt werden.⁵¹⁵ Das Bundesverfassungsgericht hat sich in seinen Entscheidungen zum Sicherheitsrecht daher wiederholt auf die Rechtsprechung des EGMR bezogen.⁵¹⁶

Darüber hinaus nimmt die EMRK in ihrer Auslegung durch den EGMR Einfluss auf die Bedeutung und Tragweite der Grundrechte in der EU-Grundrechtecharta, Art. 52 Abs. 3 GRCh.⁵¹⁷

⁵¹¹ Hoffmann-Riem, Deutscher Bundestag, 1. Untersuchungsausschuss 2014, S. 10.

⁵¹² Vgl. zu dem ebenfalls einschlägigen Art. 17 Abs. 1 IPbPR, Winter, Kohärenz des Nachrichtendienstrechts, S. 341, der aber „keine höheren Anforderungen stellt als das vom EGMR entwickelte, präzise Menschenrechtsregime“ (ebd.) und daher ausgeklammert wird.

⁵¹³ Meyer-Ladewig/Raumer/Nettesheim/Meyer-Ladewig/Nettesheim, Einleitung Rn. 15.

⁵¹⁴ BVerfG, Beschluss v. 14.10.2004 - 2 BvR 1481/04 - Rn. 31; Meyer-Ladewig/Raumer/Nettesheim/Meyer-Ladewig/Nettesheim, Einleitung Rn. 18.

⁵¹⁵ BVerfG, Beschluss v. 14.10.2004 - 2 BvR 1481/04 - Rn. 30 ff.; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 97; Steiner, GSZ 2024, 32, 33.

⁵¹⁶ U.a. in BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 111, 280; BVerfG, Beschluss v. 27.5.2020 - 1 BvR 1873/13 - 1 BvR 2618/13 - Rn. 253; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 214.

⁵¹⁷ Jarass, Art. 52 GrCh Rn. 65; Schwander, Extraterritoriale Wirkung, S. 92.

2. *Einschlägiges Konventionsrecht*

Für das Nachrichtendienstrecht relevant ist vor allem Art. 8 EMRK.⁵¹⁸ Dieser schützt das Privat- und Familienleben, die Wohnung und die Korrespondenz. Die Begriffe „Privatleben“ und „Korrespondenz“ werden weit ausgelegt.⁵¹⁹

Der Begriff des „Privatlebens“ kann nicht abschließend definiert werden. Er schützt das Recht zu persönlicher Entwicklung bezogen auf die Persönlichkeit und persönliche Autonomie, davon erfasst ist auch das Recht, ein „privates Sozialleben“ zu führen, also beispielsweise Beziehungen zu etablieren.⁵²⁰

Der Begriff der Korrespondenz schützt unter anderem auch Telekommunikationsgespräche.⁵²¹

Wenn der Staat private Daten systematisch sammelt, speichert, verarbeitet und verwertet, ist der Anwendungsbereich von Art. 8 EMRK eröffnet.⁵²² Der Schutzbereich von Art. 8 EMRK ist weit, seine Garantien werden nach deutschem Recht von unterschiedlichen Grundrechten verbürgt.⁵²³

Art. 8 Abs. 2 EMRK enthält Anforderungen, die für die Eingriffsrechtfertigung erfüllt sein müssen. Demnach muss der Eingriff auf einer gesetzlichen Grundlage erfolgen und in einer demokratischen Gesellschaft für die nationale oder öffentliche Sicherheit, das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig sein.

Daneben ist Art. 10 EMRK, der die Meinungsfreiheit schützt, unter anderem im Zusammenhang mit nachrichtendienstlichen Maßnahmen gegenüber Journalistinnen eröffnet.⁵²⁴ Die Eingriffsrechtfertigung bestimmt sich hier nach Art. 10 Abs. 2 EMRK.

⁵¹⁸ Dessen Abs. 1 lautet: „(1) Jede Person hat das Recht auf Achtung ihres Privat/ und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.“

⁵¹⁹ *Breuer*, § 25 Datenschutz, 549, 557, Rn. 23; *Jarass*, Art. 7 GrCh Rn. 13; *Ní Loideain*, EU Data Privacy Law and Serious Crime, S. 33.

⁵²⁰ EGMR 5.9.2017 (GK) – 61496/08 Rn. 70 – *Barbulescu/Rumänien*.

⁵²¹ EGMR 6.9.1978 – 5029/71 Rn. 41 – *Klass und andere gg. Deutschland*; *Huber*, Nachrichtendienste und EMRK 2019, 191, 193; in der jüngeren Rechtsprechung untersucht stellt der EGMR jedoch (nur) auf eine Beeinträchtigung des Privatlebens ab, *Ní Loideain*, EU Data Privacy Law and Serious Crime, S. 39.

⁵²² *Karpenstein/Mayer/Pätzold*, Art. 8 Rn. 77; EGMR 30.1.2020 – 50001/12 Rn. 75 – *Breyer gegen Deutschland*: “Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.”

⁵²³ *Steiner*, GSZ 2024, 32, 33.

⁵²⁴ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 451 – *Big Brother Watch gg. UK*; EGMR 29.6.2006 – 54934/00 Rn. 143-145 – *Weber und Saravia gg. Deutschland*.

Außerdem ist gegebenenfalls das Recht auf wirksame Beschwerde gem. Art. 13 EMRK einschlägig.⁵²⁵

3. Extraterritoriale Wirkung der EMRK

Für nachrichtendienstliche Tätigkeiten, die Personen im Inland betreffen, ist die EMRK anwendbar.⁵²⁶

Demgegenüber ist umstritten, ob die EMRK Geltung entfaltet, wenn die Maßnahme Personen außerhalb des Staatsgebiets trifft. Art. 1 EMRK ordnet an, dass die in Abschnitt 1 der EMRK verliehenen Rechte nur den der Hoheitsgewalt der jeweiligen Vertragspartei unterstehenden Personen zugesichert werden. Vor diesem Hintergrund könnte die EMRK bei Maßnahmen der Nachrichtendienste, die Ausländer im Ausland zum Ziel haben, mangels einer Ausübung von Hoheitsgewalt gegenüber diesen Personen nicht anwendbar sein. Relevant ist dies unter anderem für die strategische Ausland-Fernmeldeaufklärung und für Eingriffe in informationstechnische Systeme von Ausländern im Ausland gem. § 34 ff. BNDG. Die Problematik stellt sich aber auch bei anderen Maßnahmen des BND und des BfV oder MAD, soweit sie Ausländer im Ausland beobachten.

Grundsätzlich geht der EGMR davon aus, dass die EMRK nicht extraterritorial wirkt. Von diesem Grundsatz sind jedoch Ausnahmen anerkannt. So wird die Ausübung von Hoheitsgewalt im Sinne des Art. 1 EMRK bejaht, wenn ein Staat die grundsätzliche Kontrolle über ein Territorium oder die individuelle Kontrolle über einen Sachverhalt ausübt. Die grundsätzliche Kontrolle für ein Gebiet wird bejaht, wenn ein Staat zu Maßnahmen greift, die dort „üblicherweise der Regierung vorbehalten“ sind, insbesondere „militärische Macht“. Bei der individuellen Kontrolle eines Staates über einen Sachverhalt im Ausland hat der EGMR drei Fallgruppen anerkannt: Die individuelle Kontrolle wird bejaht, wenn der tätigwerdende Staat mit dem gastgebenden Staat abgesprochen hat, seine Staatsgewalt dort so „wie im Inland“ auszuüben, wenn er dort diplomatisch oder konsularisch tätig wird oder wenn er einen „sonstigen Grundrechtseingriff“ vornimmt, der durch seine „Amtsträger (...) beherrscht wird“.⁵²⁷

Bei der Erhebung elektronischer Kommunikation übt ein Staat jedoch keine physisch kontrollierte, sondern lediglich „virtuelle“ Gewalt aus, was gegen eine Subsumtion unter die Ausnahmeklausel und somit gegen die Anwendbarkeit der EMRK spricht.⁵²⁸

⁵²⁵ *Venedig-Kommission*, Report 2015, Rn. 90.

⁵²⁶ *Talmon*, JZ 2014, 783, 785.

⁵²⁷ *Schwander*, Extraterritoriale Wirkung, S. 106 ff., 111; EGMR 7.7.2011 – 55721/07 Rn. 133 ff., 138 – Al-Skeini; Karpenstein/Mayer/*Johann*, Art. 1 EMRK Rn. 20 ff.; *Talmon*, JZ 2014, 783, 784.

⁵²⁸ *Talmon*, JZ 2014, 783, 784; *Gärditz*, JZ 2020, 825, 827; *Schneider*, Fernmeldegeheimnis, S. 197 f.

Andererseits wird für die Anwendbarkeit der EMRK vorgebracht, dass kein Fall der Extraterritorialität vorläge, da die nachrichtendienstliche Tätigkeit technisch vom Territorium des Konventionsstaates ausgehe, auch wenn die Datenerhebung auf einem anderen Staatsgebiet erfolge.⁵²⁹ Dieses Argument deckt jedoch nicht alle Konstellationen ab, da die technische Umsetzung andernorts erfolgen kann.

Darüber hinaus wird argumentiert, dass zwar keine der etablierten Fallgruppen einer Ausnahme vom Grundsatz der Territorialität einschlägig sei, sich aus der Rechtsprechung des EGMR aber ableiten ließe, dass eine Vertragspartei, die „für sich in Anspruch nimmt, außerhalb ihres Hoheitsgebiets (...) Überwachungsmaßnahmen durchzuführen, (...) ‚einen Teil der öffentlichen Gewalt‘ ausübt, der ‚normalerweise von der Regierung eines anderen Staates ausgeübt wird‘ (...) und auf diese Weise einen hinreichenden Anhaltspunkt dafür schafft, dass Betroffene in gleicher Weise ihrer Jurisdiktion unterliegen wie dies bei Maßnahmen des Aufenthaltsstaates der Fall wäre.“⁵³⁰

Die Rechtsprechung des EGMR erlaubte bisher keine eindeutigen Schlüsse, welche dieser Linien er vertrat.⁵³¹ Das liegt auch daran, dass der EGMR die Anwendbarkeit nur prüft, wenn die Nichtanwendbarkeit aktiv gerügt wurde⁵³². So hat das Gericht unter anderem über Massenüberwachungsregime aus dem Vereinigten Königreich und Schweden entschieden, weshalb man vermuten könnte, dass es die Anwendbarkeit der EMRK bejaht. Allerdings ist in diesen Fällen entweder die Unanwendbarkeit der EMRK nicht gerügt worden oder die Maßnahmen waren ohnehin gerechtfertigt.⁵³³

In der Entscheidung *Wieder and Guarnieri v. UK* hat der EGMR jedoch entschieden, dass der Anwendungsbereich der EMRK bei der Überwachung elektronischer Kommunikation auch dann eröffnet ist, wenn der Betroffene sich außerhalb des Staatsgebiets befindet. Entscheidend sei nicht, wo der Betroffene sich aufhalte, sondern wo die Datenverarbeitung erfolge: Der Eingriff würde dort stattfinden, wo die Kommunikation „abgefangen, gefiltert, geprüft und genutzt“ wird. Da diese Verarbeitungen im Vertragsstaat erfolgen, sei der Anwendungsbereich eröffnet. Ob die in der Rechtsprechung anerkannten Ausnahmen vom Grundsatz der Territorialität einschlägig sind, müsse deshalb nicht geprüft werden.⁵³⁴

⁵²⁹ *Schmahl*, JZ 2014, 220, 227.

⁵³⁰ Mit Verweis auf EGMR 7.7.2011 – 55721/07 Rn. 149 – Al Skeini, Karpenstein/Mayer/Johann, Art. 1 EMRK Rn. 35.

⁵³¹ So auch Vogt, der dies ausführlich untersucht, *Vogt*, Strategische Auslands-telekommunikationsüberwachung, S. 590.

⁵³² *Schwander*, Extraterritoriale Wirkung, S. 105.

⁵³³ Zu den Kammerentscheidungen *Gärditz*, JZ 2020, 825, 827; auch in der Entscheidung EGMR 29.6.2006 – 54934/00 – Weber und Saravia gg. Deutschland zur deutschen strategischen Überwachungen nach G 10, hat der EGMR sich zur Anwendbarkeit nicht geäußert, weil die Beschwerden ohnehin „aus anderen Gründen erfolglos“ gewesen seien, *Schwander*, Extraterritoriale Wirkung, S. 104; Karpenstein/Mayer/Johann, Art. 1 EMRK Rn. 35.

⁵³⁴ EGMR 12.12.2023 – 64371/16, 64407/17 Rn. 93 ff. – *Wieder and Guarnieri v. UK*.

Wenn die Verarbeitung der elektronischen Kommunikation aus einem Vertragsstaat heraus gesteuert wird, ist der Anwendungsbereich der EMRK somit eröffnet. Wenn die gesamte Datenverarbeitung allein im Ausland stattfindet, beispielsweise durch den BND und die Bundeswehr im Auslandseinsatz, wäre der Anwendungsbereich nach der neuesten Rechtsprechung des EGMR eigentlich zu verneinen. Da die erhobenen Daten in der Regel im Vertragsstaat gespeichert und genutzt werden, ist aber davon auszugehen, dass der Anwendungsbereich der EMRK bei elektronischer Überwachung dennoch stets eröffnet ist.

Ungeklärt ist, ob die EMRK in Sachverhalten anwendbar ist, in denen Ausländer im Ausland analog überwacht werden, beispielsweise durch Observationen. Für die Anwendbarkeit der EMRK in diesen Situationen spricht, dass es sich um Grundrechtseingriffe handelt, die vom Vertragsstaat „beherrscht“ werden, weshalb die Ausnahme vom Grundsatz der Territorialität einschlägig ist, nach der die individuelle Kontrolle eines Vertragsstaates über einen Sachverhalt für die Eröffnung des Anwendungsbereichs ausreichend ist⁵³⁵.

4. Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte

Der Europäische Gerichtshof für Menschenrechte (EGMR) entscheidet über die Auslegung der EMRK (Art. 32 EMRK). Seine Urteile sind für den Mitgliedstaat, dessen Recht er untersucht hat, bindend (Art. 46 EMRK).⁵³⁶ Aus seiner Rechtsprechung lassen sich einige Mindestanforderungen⁵³⁷ für ein konventionskonformes Kontrolldesign nachrichtendienstlicher Maßnahmen ableiten.

Huber resümiert zwar zutreffend, dass das G 10 „die Bewährungsprobe vor den Vorgaben der EMRK weitgehend bestanden hat.“⁵³⁸ Es muss jedoch betont werden, dass der EGMR bisher nicht über andere deutsche Nachrichtendienstgesetze und Kontrollleure zu entscheiden hatte und die beiden zu Deutschland ergangenen Urteile, *Klass* und *Weber gegen Deutschland*, bereits Jahrzehnte zurückliegen⁵³⁹. Seitdem hat der

⁵³⁵ Vgl. [Teil 2 B.I. 3.](#)

⁵³⁶ *Cameron*, Oversight of Intelligence Agencies, 71, 77 f.

⁵³⁷ *Venedig-Kommission*, Report 2015, Rn. 85: “To begin with, it should be recollected that the European Convention on Human Rights consists of minimum standards. Thus, the Court’s case law is only a point of departure for European states”.

⁵³⁸ *Huber*, Nachrichtendienste und EMRK, 191, 197.

⁵³⁹ EGMR 6.9.1978 – 5029/71 Rn. 42 – *Klass* und andere gg. Deutschland; EGMR 29.6.2006 – 54934/00 Rn. 105 – *Weber* und *Saravia* gg. Deutschland.

EGMR seine Rechtsprechung erheblich weiterentwickelt. Wenn die deutschen Nachrichtendienstgesetze jetzt durch den EGMR überprüft würden, würde das Ergebnis weniger positiv ausfallen.⁵⁴⁰

Zur Kontrolle nachrichtendienstlicher Befugnisse hat sich das Gericht im Rahmen der Prüfung der Voraussetzungen von Art. 8 Abs. 2 EMRK geäußert, meistens die Frage betreffend, ob die gesetzliche Regelung als „in einer demokratischen Gesellschaft notwendig“ erachtet werden kann.⁵⁴¹ Inhaltlich hat diese Tatbestandsvoraussetzung Ähnlichkeit mit der deutschen Verhältnismäßigkeitsprüfung.⁵⁴² Wie sie ihre nationale Sicherheit am besten schützen, können die Konventionsstaaten im Rahmen eines Beurteilungs- und Ermessenspielraums eigenständig entscheiden („(wide) margin of appreciation“).⁵⁴³ Allerdings kontrolliert der EGMR die Ausgestaltung dieses Spielraums, sowohl bezogen auf die Gesetzgebung als auch auf die Gesetzesanwendung.⁵⁴⁴ Der EGMR setzt in diesem Zusammenhang voraus, dass „ausreichende und angemessene Garantien gegen Missbrauch“ etabliert sind („Missbrauchsfestigkeit“⁵⁴⁵).⁵⁴⁶ Diese Schutzmechanismen seien notwendig, weil ein System geheimer Überwachung zum Schutz der nationalen Sicherheit das Risiko birgt, die Demokratie zu zerstören, obwohl es errichtet wurde, um sie zu beschützen.⁵⁴⁷ Ob ausreichende Schutzmechanismen vorgesehen sind, entscheidet der EGMR unter anderem anhand einer Gesamtbetrachtung

⁵⁴⁰ Vgl. [Teil 3 B. II. 1. b.](#); [Teil 3 C. II. 1. a. aa](#)) (2); zum BNDG *Steiner*, GSZ 2024, 32.

⁵⁴¹ EGMR 6.9.1978 – 5029/71 Rn. 42 – Klass und andere gg. Deutschland; EGMR 29.6.2006 – 54934/00 Rn. 105 – Weber und Saravia gg. Deutschland; EGMR 18.5.2010 – 26839/05 Rn. 153 f. – Kennedy gg. UK; EGMR 4.12.2015 – 47143/06 Rn. 227, 232 – Roman Zakharov gg. Russland; EGMR 2.1.2016 – 37138/14, Rn. 55, 57 – Szabó und Vissy gg. Ungarn; EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 339 – Big Brother Watch gg. UK; teilweise auch bei der Prüfung, ob der Eingriff „gesetzlich vorgesehen“ i.S. v. Art. 8 Abs. 2 EMRK war, wobei u.a. zu prüfen ist, ob die Norm „zugänglich“, „vorhersehbar“ und mit dem Rechtsstaatsprinzip vereinbar ist, vgl. EGMR 28.6.2007 – 62540/00 Rn. 71, 93 – Assoc. For European Integration and Human Rights and Ekimdzhiyev gg. Bulgarien; *Ní Loideain* kritisiert, dass der EGMR in der neueren Rechtsprechung nicht mehr sauber zwischen den unterschiedlichen Tatbestandsvoraussetzungen von Art. 8 Abs. 2 EMRK differenziert, *Ní Loideain*, EU Data Privacy Law and Serious Crime, S. 67 ff.

⁵⁴² *Aust*, AVR 2014, 375, 398; *Bernstorff/Asche*, Hdb. des Rechts der Nachrichtendienste, 79, 94.

⁵⁴³ U.a. EGMR 29.6.2006 – 54934/00 Rn. 106 – Weber und Saravia gg. Deutschland; „wide“ margin of appreciation in EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 339 – Big Brother Watch gg. UK und EGMR 25.5.2021 – 35252/08 Rn. 252 – Centrum för Rättvisa gg. Schweden; *Bernstorff/Asche*, Hdb. des Rechts der Nachrichtendienste, 79, 97.

⁵⁴⁴ EGMR 4.12.2015 – 47143/06 Rn. 232 – Roman Zakharov gg. Russland.

⁵⁴⁵ *Winter*, Kohärenz des Nachrichtendienstrechts, S. 345.

⁵⁴⁶ „(...) [A]dequate and effective safeguards against abuse“, st. Rspr., vgl. EGMR 6.9.1978 – 5029/71 Rn. 50 – Klass und andere gg. Deutschland; EGMR 2.1.2016 – 37138/14, Rn. 57 – Szabó und Vissy gg. Ungarn; EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 339 – Big Brother Watch gg. UK; EGMR 25.5.2021 35252/08 Rn. 250 – Centrum för Rättvisa gg. Schweden.

⁵⁴⁷ EGMR 29.6.2006 – 54934/00 Rn. 106 – Weber und Saravia gg. Deutschland; EGMR 4.12.2015 – 47143/06 Rn. 232 – Roman Zakharov gg. Russland; EGMR 2.1.2016 – 37138/14 Rn. 57 – Szabó und Vissy gg. Ungarn; EGMR 25.5.2021 – 35252/08 Rn. 253 – Centrum för Rättvisa gg. Schweden.

folgender Kriterien: Er analysiert die für die Aufsicht zuständige Behörde sowie die Art des Rechtsbehelfs gegen die Maßnahme⁵⁴⁸ und prüft, ob die Verfahren für die Aufsicht der Anordnung und Ausführung der Maßnahme sich im Rahmen dessen bewegen, was in einer demokratischen Gesellschaft notwendig ist⁵⁴⁹.

Um die Vorgaben des EGMR zur Kontrolle heimlicher Maßnahmen detailliert darstellen zu können, muss zwischen den Kriterien für gezielte Überwachungsmaßnahmen und denen für die sog. „Massenüberwachung“ bzw. in der deutschen Terminologie der strategischen Überwachung differenziert werden, weil für letztere vergleichsweise strengere Kontrollanforderungen etabliert wurden⁵⁵⁰ (ebenso wie im deutschen Verfassungsrecht für die strategische Ausland-Fernmeldeüberwachung).

a. Standards für gezielte, personenbezogene Maßnahmen

Die Schutzmechanismen, die bei der Anwendung zielgerichteter, heimlicher Überwachungsmaßnahmen gegenüber bestimmten Personen beachtet werden müssen, hat der EGMR in einer Vielzahl von Entscheidungen ausdifferenziert. Einige der den Entscheidungen zugrundeliegenden Gesetze regeln den Einsatz heimlicher Befugnisse zum Schutz der nationalen Sicherheit und zu Zwecken der Strafverfolgung.⁵⁵¹ Das Gericht wendet ohnehin für beides identische Maßstäbe an.⁵⁵²

Als Leiturteil gilt *Klass und andere gegen Deutschland* von 1978, in dem der EGMR über die Konventionskonformität von individuellen Beschränkungen nach dem G 10 zu entscheiden hatte. Seitdem prüft der EGMR „drei Stufen“ der Kontrolle, die nach ihrem *Zeitpunkt* unterschieden werden⁵⁵³:

⁵⁴⁸ EGMR 28.6.2007 – 62540/00 Rn. 77 – Assoc. For European Integration and Human Rights and Ekimdzhiev gg. Bulgarien; EGMR 4.12.2015 – 47143/06 Rn. 232 – Roman Zakharov gg. Russland.

⁵⁴⁹ EGMR 18.5.2010 – 26839/05 Rn. 154 – Kennedy gg. UK; EGMR 4.12.2015 – 47143/06 Rn. 232 – Roman Zakharov gg. Russland; EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 339 – Big Brother Watch gg. UK.

⁵⁵⁰ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 347 – Big Brother Watch gg. UK, der EGMR differenziert zwischen den Anforderungen an gezielte Überwachungen und denen an anlasslose Überwachungen, vgl. u.a. Rn. 349 ff.: „Massenüberwachung“ zielt im Gegensatz zu gezielten Überwachungen unter anderem generell auf internationale Kommunikation ab und erfolgt nicht zu Zwecken der Strafverfolgung, sondern ausschließlich zum Schutz der nationalen Sicherheit.

⁵⁵¹ U.a. EGMR 28.6.2007 – 62540/00 Rn. 79 – Assoc. For European Integration and Human Rights and Ekimdzhiev gg. Bulgarien; EGMR 18.5.2010 – 26839/05, Rn. 159 – Kennedy gg. UK; EGMR 4.12.2015 – 47143/06 Rn. 237 – Roman Zakharov gg. Russland; EGMR 2.1.2016 – 37138/14 Rn. 55 – Szabó und Vissy gg. Ungarn.

⁵⁵² Petri, Hdb. Sicherheits- und Staatsschutzrecht, 667, 713 Rn. 110.

⁵⁵³ European Union Agency for Fundamental Rights, Surveillance by intelligence services, S. 93.

„Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated.“⁵⁵⁴

Für jede Stufe gelten bestimmte Vorgaben, die aber nicht per se verbindlich sind, sondern einander im Rahmen einer Gesamtbetrachtung unter Umständen ausgleichen können.⁵⁵⁵ Da Betroffene mindestens auf den ersten beiden Stufen keine Kenntnis von der Überwachung haben und sich deshalb nicht gerichtlich dagegen wehren können, sei essenziell, dass innerhalb des Verfahrens „angemessene und wirksame Garantien gegen Missbrauch vorgesehen sind“.⁵⁵⁶ Der EGMR begründet die Notwendigkeit für Kontrollen auf den ersten beiden Stufen also wie das Bundesverfassungsgericht: weil der Betroffene sich wegen der Heimlichkeit selbst nicht wehren kann, braucht es zur Kompensation unabhängige Kontrollen.⁵⁵⁷

Die Maßgaben zur Kontrolle erwähnt und prüft der EGMR nicht in jedem Urteil, stattdessen setzt er im Einzelfall unterschiedliche Schwerpunkte. Die folgende Zusammenstellung der Kriterien aus unterschiedlichen Entscheidungen soll eine Antwort auf die Frage bieten, welche Aspekte für ein konventionskonformes Kontrolldesign notwendig sind. Das bedeutet aber nicht zwingend, dass der EGMR jeden dieser Gesichtspunkte tatsächlich prüfen würde, wenn er ein deutsches Nachrichtendienstgesetz zu beurteilen hätte.⁵⁵⁸

⁵⁵⁴ EGMR 6.9.1978 – 5029/71 Rn. 55 – Klass und andere gg. Deutschland; EGMR 4.12.2015 – 47143/06 Rn. 233 – Roman Zakharov gg. Russland; EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 336 – Big Brother Watch gg. UK; in EGMR 28.6.2007 – 62540/00 Rn. 84 – Assoc. For European Integration and Human Rights and Ekimdzhiev gg. Bulgarien spricht das Gericht von der “Initial stage”; auch in EGMR 2.1.2016 – 37138/14, Rn. 75 – Szabó und Vissy gg. Ungarn spricht der EGMR von “stage of authorisation”. Soweit von Bernstorff/Asche vertreten, dass „der Gerichtshof in seiner Spruchpraxis nicht eindeutig zwischen präventiven Anordnungs- und Kontrollmechanismen auf der einen Seite, und nachgängigen Mechanismen der Überprüfung (...) auf der anderen“ unterscheide, vgl. *Bernstorff/Asche*, Hdb. des Rechts der Nachrichtendienste, 79, 98, ist dies in Anbetracht der wiederholten Erwähnung der drei Kontrollstufen durch das Gericht nicht nachvollziehbar.

⁵⁵⁵ EGMR 2.1.2016 – 37138/14, Rn.77 – Szabó und Vissy gg. Ungarn.

⁵⁵⁶ EGMR 6.9.1978 – 5029/71 Rn. 55 – Klass und andere gg. Deutschland; EGMR 29.6.2006 – 54934/00 Rn. 106 – Weber und Saravia gg. Deutschland; EGMR 4.12.2015 – 47143/06 Rn. 232 – Roman Zakharov gg. Russland.

⁵⁵⁷ *Petri*, Hdb. Sicherheits- und Staatsschutzrecht, 667, 715 Rn. 117; vgl. [Teil 2 A. I. 3. a.](#)

⁵⁵⁸ Vgl. [Teil 2 B. I. 4. a. dd\).](#)

aa) Ex ante-Genehmigung

Auf der ersten der drei Stufen muss die Anordnung („warrant“), auf deren Grundlage eine Zielperson heimlich überwacht werden soll, zunächst ex ante genehmigt werden (*Zeitpunkt*).⁵⁵⁹

Der für die Genehmigung zuständige *Kontrolleur* muss „ausreichend unabhängig von der Exekutive“ sein⁵⁶⁰, wobei der EGMR richterliche Vorabkontrollen präferiert⁵⁶¹. Die richterliche Kontrolle sei am besten geeignet, Unabhängigkeit, Unparteilichkeit und ein ordnungsgemäßes Verfahren zu garantieren.⁵⁶²

Im Rahmen der Prüfung, ob die Einrichtung hinreichend unabhängig von der Exekutive ist, sind die „Art der Ernennung“ und der „rechtliche Status der Mitglieder“ entscheidend (*Distanz*). Konventionskonform sei beispielsweise die Ernennung des Kontrolleurs durch das Parlament oder den Regierungschef. Der unabhängige Status wurde bejaht, soweit die kontrollierenden Institutionen sich aus Mitgliedern von Regierungsfraktion und Opposition oder aus zum Richteramt befähigten Juristen zusammensetzten. Demgegenüber hat das Gericht die Kontrolle durch einen Minister oder durch Staatsanwälte als nicht ausreichend unabhängig beurteilt.⁵⁶³

Sollte der Kontrolleur nicht unabhängig sein, ist die Konventionswidrigkeit trotzdem abwendbar: Soweit die Schutzvorkehrungen auf der zweiten und dritten Stufe (während der Durchführung und nach Abschluss der Maßnahme) höher sind, können diese die Defizite auf der ersten Stufe ausgleichen.⁵⁶⁴ Die genehmigende Einrichtung

⁵⁵⁹ St. Rspr. seit EGMR 6.9.1978 – 5029/71 Rn. 56 – Klass und andere gg. Deutschland.

⁵⁶⁰ EGMR 4.12.2015 – 47143/06 Rn. 258 – Roman Zakharov gg. Russland; in Klass und andere gg. Deutschland und Weber und Saravia gg. Deutschland hatte der EGMR festgestellt, dass die Genehmigung durch die G 10-Kommission konventionskonform ist, vgl. EGMR 29.6.2006 – 54934/00 Rn. 117 – Weber und Saravia gg. Deutschland.

⁵⁶¹ EGMR 6.9.1978 – 5029/71 Rn. 56 – Klass und andere gg. Deutschland; EGMR 18.5.2010 – 26839/05, Rn. 167 – Kennedy gg. UK; Richterliche Kontrolle als „best practice“, *Ní Loideain*, EU Data Privacy Law and Serious Crime, S. 55; *Venedig-Kommission*, Report 2007, Rn. 200.

⁵⁶² EGMR 6.9.1978 – 5029/71 Rn. 55 – Klass und andere gg. Deutschland.

⁵⁶³ EGMR 4.12.2015 – 47143/06 Rn. 278 – Roman Zakharov gg. Russland; die Kontrolle durch einen Justizminister sei „politische Kontrolle“ und daher „von Natur aus nicht in der Lage“ die Verhältnismäßigkeit zu prüfen, EGMR 2.1.2016 – 37138/14, Rn. 75 – Szabó und Vissy gg. Ungarn; die G 10-Kommission wird dementsprechend als ausreichend unabhängig eingeordnet, vgl. EGMR 6.9.1978 – 5029/71 Rn. 56 – Klass und andere gg. Deutschland.

⁵⁶⁴ *Venedig-Kommission*, Report 2015, Rn. 106: „Whatever the case, if a holistic approach is taken, assessing the system as a whole, then it seems clear that where a system lacks independent controls at the authorisation stage, this should mean that very strong safeguards must exist at the follow-up/oversight stage, for example, the power to take binding decisions“.

muss dann ihrerseits der Kontrolle eines Richters oder einer vergleichbar unabhängigen Institution unterliegen.⁵⁶⁵

In Eilfällen, in denen die Genehmigung durch ein Gericht oder eine unabhängige Einrichtung die Maßnahme so verzögern würde, dass ihr Zweck vereitelt würde, kann von der vorherigen Genehmigung abgesehen werden. Dies ist jedoch nur in „seltenen, hinreichend begründeten Fällen“ möglich. Ob ein Eilfall vorlag und die Daten gespeichert werden dürfen, muss nachträglich richterlich (oder durch „eine vergleichbar unabhängige Stelle“⁵⁶⁶) bestätigt werden. In *Szabo und Vissy gegen Ungarn* hatte der EGMR eine Zeitspanne von 72 Stunden ohne Genehmigung als noch konventionskonform erachtet.⁵⁶⁷

Aus der Ausnahme für Eilfälle ergibt sich im Umkehrschluss, dass stets eine Genehmigung erteilt werden muss (*Modalität*).⁵⁶⁸ In der Genehmigung sollen die Personen, gegenüber denen die Maßnahme angewandt wird, oder die Voraussetzungen, auf deren Grundlage genehmigt wird, benannt werden.⁵⁶⁹

Initiativberechtigt sind bei der Vorabkontrolle die antragsstellenden Behörden. Diese müssen dem Kontrolleur alle Dokumente und Fakten vorlegen, die er benötigt, um prüfen zu können, ob ein begründeter Verdacht gegenüber dem Betroffenen vorliegt und die Maßnahme in einer demokratischen Gesellschaft notwendig ist (*Kontrollmittel zur Informationsgewinnung*)⁵⁷⁰.

Die Vorlagepflicht erstreckt sich auf geheimhaltungsbedürftige Inhalte wie beispielsweise Informationen über geheime Mitarbeiter. Diese Informationen dürften dem Kontrolleur nicht vorenthalten werden, da Geheimhaltungserfordernissen mit

⁵⁶⁵ Wobei diese Ausnahme nicht für geheime Überwachungen der Medien gelten soll, EGMR 2.1.2016 – 37138/14, Rn. 77 – Szabó und Vissy gg. Ungarn m. Verw. auf EGMR 18.5.2010 – 26839/05, Rn. 167 – Kennedy gg. UK; Ní Loideain bezeichnet es als „flexiblen Ansatz“ gegenüber der ex ante Kontrolle, *Ní Loideain*, EU Data Privacy Law and Serious Crime, S. 55; In seinem ablehnenden Votum zum Mehrheitsvotum in Szabo und Vissy gg. Ungarn kritisiert Richter Albuquerque zutreffend: „The shortcomings in the external political control are correctly criticised by the Chamber, but the judgment’s reasoning omits a holistic assessment of the subsequent surveillance review procedure, which is essential to assess if the overall fairness of the system put in place by the Hungarian legislature compensates for the shortcomings in the first stage of the secret intelligence gathering procedure“, EGMR 2.1.2016 – 37138/14 Sondervotum Rn. 25 – Szabó und Vissy gg. Ungarn.

⁵⁶⁶ So ergänzend Huber, NVwZ 2017, 1513, 1514.

⁵⁶⁷ EGMR 4.12.2015 – 47143/06 Rn. 266 – Roman Zakharov gg. Russland m. Verw. auf EGMR 28.6.2007 – 62540/00 Rn. 16, 80, 82 – Assoc. For European Integration and Human Rights and Ekimdzhiiev gg. Bulgarien; Huber, NVwZ 2017, 1513, 1514.

⁵⁶⁸ In Klass gg. Deutschland entschied der EGMR, die Kontrolle durch die G 10-Kommission sei unter anderem deshalb noch konventionskonform, weil sie ständig erfolge, EGMR 6.9.1978 – 5029/71 Rn. 56 – Klass und andere gg. Deutschland.

⁵⁶⁹ EGMR 4.12.2015 – 47143/06 Rn. 264 – Roman Zakharov gg. Russland.

⁵⁷⁰ EGMR 2.1.2016 – 37138/14 Rn. 71 – Szabó und Vissy gg. Ungarn; EGMR 4.12.2015 – 47143/06 Rn. 261 – Roman Zakharov gg. Russland.

Hilfe bestimmter Techniken (z.B. durch In-Camera-Verfahren) entsprochen werden kann.⁵⁷¹

Die Kontrolleure entscheiden darüber, ob eine heimliche Maßnahme erfolgen darf oder nicht (*Kontrollergebnisse*).

Zur *Fachkompetenz* und den *Ressourcen* der Vorabkontroll-Institution hat sich das Gericht nicht detailliert geäußert, aber festgelegt, dass der Kontrolleur mit ausreichend Macht und Kompetenzen ausgestattet sein muss, um „effektiv“ kontrollieren zu können.⁵⁷²

bb) Kontrolle während der Durchführung der Maßnahme

Zur zweiten Stufe der Kontrolle hat sich der EGMR insgesamt weniger ausführlich geäußert, weshalb die Mitgliedstaaten hier über einen größeren Gestaltungsspielraum verfügen.

Dass die kontrollierende Einrichtung unabhängig von der ausführenden Behörde sein muss, gilt auch für die Kontrolle während der Durchführung der Maßnahme (*Distanz*).⁵⁷³ Als Beispiele für unabhängige Kontrolleure nennt der EGMR Parlamentsausschüsse, Kommissare mit Befähigung zum Richteramt oder ein Gremium hochqualifizierter Richter.⁵⁷⁴ Bei einer Kontrollinstitution, deren Mitglieder auf Zeit berufen sind und die anschließend auf ihre vorige Position zurückkehren können, drohen Interessenkonflikte, die die Unabhängigkeit des Kontrolleurs gefährden, vor allem, wenn es sich dabei um Mitarbeiter aus den Nachrichtendiensten handelt.⁵⁷⁵

Die *Modalität* der Kontrollen auf der zweiten Stufe kann nach Ansicht des EGMR unterschiedlich sein, das heißt sowohl laufend als auch stichprobenartig erfolgen. In *Klass gegen Deutschland* hat das Gericht die erste und zweite Stufe gemeinsam erläutert und positiv hervorgehoben, dass die Kontrollen „ständig“ stattfinden.⁵⁷⁶ Später, in *Kennedy gegen UK*, war die halbjährige, stichprobenartige Kontrolle durch den Intercep-

⁵⁷¹ EGMR 4.12.2015 – 47143/06 Rn. 261 – Roman Zakharov gg. Russland.

⁵⁷² EGMR 6.9.1978 – 5029/71 Rn. 55 – Klass und andere gg. Deutschland; EGMR 4.12.2015 – 47143/06 Rn. 275 – Roman Zakharov gg. Russland.

⁵⁷³ EGMR 28.6.2007 – 62540/00 Rn. 85 – Assoc. For European Integration and Human Rights and Ekimdzhiev gg. Bulgarien; EGMR 2.1.2016 – 37138/14, Rn. 75 – Szabó und Vissy gg. Ungarn.

⁵⁷⁴ EGMR 28.6.2007 – 62540/00 Rn. 87 – Assoc. For European Integration and Human Rights and Ekimdzhiev gg. Bulgarien.

⁵⁷⁵ EGMR 11.4.2022 – 70078/12 Rn. 339 – Ekimdzhiev und andere gg. Bulgarien.

⁵⁷⁶ EGMR 6.9.1978 – 5029/71 Rn. 56 – Klass und andere gg. Deutschland.

tion of Communications Commissioner (Commissioner) kein Anlass, die Konventionskonformität des Überwachungsregimes zu verneinen; im Gegenteil hob der EGMR hervor, dass die Kontrolle des Commissioners „von besonderer Bedeutung“ sei.⁵⁷⁷

Der EGMR hat wiederholt betont, wie wichtig es für die Effektivität der Kontrollen ist, dass die handelnden Behörden die Anwendung geheimer Überwachungsmaßnahmen detailliert dokumentieren.⁵⁷⁸ Spiegelbildlich hierzu muss dem Kontrolleur Zugang zu allen relevanten Unterlagen gewährt werden, auch zu solchen, die Verschlusssachen sind (*Kontrollmittel zur Informationsgewinnung*).⁵⁷⁹ Nach der britischen Rechtslage, wie sie in *Kennedy gegen UK* beschrieben wurde, konnte der Commissioner die Behörden besuchen, vor Ort Dokumente sichten und mit den Beamten diskutieren.⁵⁸⁰ Der EGMR hebt diese Befugnisse in seinen Urteilsgründen jedoch nicht hervor.

Die *Kontrollergebnisse* bei Verstößen seien ein wichtiges Element, um beurteilen zu können, ob die Kontrollen effektiv sind, betonen die Richter in *Roman Zakharov gegen Russland*. Die Kontrolleure müssten rechtswidrige Datenverarbeitungen stoppen können und anordnen dürfen, dass rechtswidrig erlangtes Material zerstört wird.⁵⁸¹

Zur *Fachkompetenz* hat sich das Gericht in *Ekimdzhiev und andere gg. Bulgarien* geäußert, indem es kritisiert hat, dass nur eines von fünf Mitgliedern der kontrollierenden Institution juristisch ausgebildet und erfahren war.⁵⁸²

Inhaltlich erstreckt sich die Prüfung auf der zweiten Stufe auf unterschiedliche Aspekte wie beispielsweise die Fragen, ob die Behörden entsprechend den Anforderungen der Genehmigung agiert haben, die erhobenen Daten in der schriftlichen Dokumentation richtig wiedergegeben werden oder ob diese innerhalb des angegebenen Zeitraums zerstört wurden (*Kontrolltiefe*).⁵⁸³

⁵⁷⁷ EGMR 18.5.2010 – 26839/05 Rn. 166 – Kennedy gg. UK.

⁵⁷⁸ EGMR 18.5.2010 – 26839/05 Rn. 165 – Kennedy gg. UK; „particularly important“, EGMR 4.12.2015 – 47143/06 Rn. 272 – Roman Zakharov gg. Russland; *Ni Loideain*, EU Data Privacy Law and Serious Crime, S. 54.

⁵⁷⁹ EGMR 4.12.2015 – 47143/06 Rn. 281 – Roman Zakharov gg. Russland mit Verweis auf Kennedy Rn. 166, in der die britische Rechtslage auf der zweiten Stufe beschrieben wird, die der EGMR als konventionskonform erachtet hatte; EGMR 11.4.2022 – 70078/12 Rn. 343 – Ekimdzhiev und andere gg. Bulgarien.

⁵⁸⁰ EGMR 18.5.2010 – 26839/05, Rn. 60 – Kennedy gg. UK, Bericht des Commissioners aus 2005-2006.

⁵⁸¹ EGMR 4.12.2015 – 47143/06 Rn. 282 – Roman Zakharov gg. Russland mit Verweis EGMR 6.9.1978 – 5029/71 Rn. 53 – Klass und andere gg. Deutschland, wo rechtswidrige Verarbeitungen beendet werden mussten, und EGMR 18.5.2010 – 26839/05, Rn. 168, Kennedy gg. UK, wo der Commissioner die Zerstörung anordnen konnte; EGMR 11.4.2022 – 70078/12 Rn. 344 – Ekimdzhiev und andere gg. Bulgarien.

⁵⁸² EGMR 11.4.2022 – 70078/12 Rn. 342 – Ekimdzhiev und andere gg. Bulgarien.

⁵⁸³ EGMR 28.6.2007 – 62540/00 Rn. 85 – Assoc. For European Integration and Human Rights and Ekimdzhiev gg. Bulgarien; EGMR 4.12.2015 – 47143/06 Rn. 274 – Roman Zakharov gg. Russland.

Der EGMR betont zudem, dass es entscheidend ist, dass der Kontrolleur selbst von der Öffentlichkeit kontrolliert wird. Dieses Erfordernis kann unter anderem mit einem Tätigkeitsbericht gegenüber dem Parlament oder der Öffentlichkeit umgesetzt werden.⁵⁸⁴

Darüber hinaus sei es trotz der notwendigen Geheimhaltung nicht unmöglich, den Betroffenen bereits auf der zweiten Stufe einen beschränkten Rechtsbehelf zu verleihen: So seien Verhandlungen möglich, in denen der Betroffene nicht erfährt, ob er tatsächlich überwacht wurde. Als Beispiel nennt der EGMR unter anderem das Beschwerderecht zur G 10-Kommission.⁵⁸⁵

cc) Ex post-Kontrolle

Die dritte Stufe betrifft die Kontrolle, nachdem die Maßnahme beendet wurde. Wenn Betroffene sich gerichtlich gegen eine Maßnahme wehren möchten, müssen sie zunächst Kenntnis von der Maßnahme haben. Sie erfahren in der Regel jedoch nur davon, wenn die überwachende Behörde sie benachrichtigt. Der EGMR erachtet es als konventionskonform, wenn Betroffene erst dann in Kenntnis gesetzt werden, wenn der Zweck der Maßnahme dadurch nicht mehr vereitelt werden kann. Demgegenüber sei es konventionswidrig, wenn gar keine Benachrichtigung gegenüber Betroffenen vorgesehen ist. Alternativ zur Benachrichtigung könne ein Rechtsweg eingeführt werden, bei dem eine tatsächliche Betroffenheit nicht nachgewiesen werden muss und der somit unabhängig von einer Benachrichtigung möglich ist.⁵⁸⁶

Der EGMR etabliert die mitgliedstaatlichen Gerichte als *Kontrollleure*, lässt es alternativ aber zu, dass eine unabhängige Einrichtung mit der Prüfung betraut wird. So betont das Gericht in *Kennedy und andere gg UK*, dass das Investigatory Powers Tribunal (IPT) eine unabhängige, unparteiische, mit eigenem Verfahrensrecht ausgestattete Einrichtung sei. Dessen Mitglieder seien entweder hochrangige Richter oder erfahrene Anwälte. Das IPT habe Zugang zu Verschlusssachen und könne die Beendigung einer

⁵⁸⁴ EGMR 4.12.2015 – 47143/06 Rn. 282 – Roman Zakharov gg. Russland mit Verweis auf unter anderem *Kennedy gg. UK*, Rn. 166.

⁵⁸⁵ EGMR 28.6.2007 – 62540/00 Rn. 100 – Assoc. For European Integration and Human Rights and Ekimdzhiev gg. Bulgarien.

⁵⁸⁶ EGMR 28.6.2007 – 62540/00 Rn. 101 f. – Assoc. For European Integration and Human Rights and Ekimdzhiev gg. Bulgarien; EGMR 18.5.2010 – 26839/05, Rn. 167 – *Kennedy gg. UK*; EGMR 4.12.2015 – 47143/06 Rn. 287 f. – Roman Zakharov gg. Russland; EGMR 2.1.2016 – 37138/14, Rn. 86 – Szabó und Vissy gg. Ungarn.

Maßnahme, die Zerstörung rechtswidrigen Materials und die Zahlung von Entschädigungen anordnen. Positiv bewertet der EGMR, dass die Entscheidungen des IPT veröffentlicht werden.⁵⁸⁷

dd) Drei Stufen-Kontrolle: Leitbild oder zwingende Vorgabe?

Die Rechtsprechung des EGMR zur Kontrolle nachrichtendienstlicher Befugnisse ist im Gegensatz zu der des Bundesverfassungsgerichts schwieriger zu systematisieren. Denn der EGMR hat mit der dreistufigen Kontrolle zwar ebenfalls allgemeine, über den Einzelfall hinaus geltende Anforderungen an die Kontrolle für eine verhältnismäßige Durchführung personenbezogener, heimlicher Maßnahmen durch Nachrichtendienste formuliert, diese sind aber – im Gegensatz zu den Vorgaben des Bundesverfassungsgerichts zu eingriffsintensiven Maßnahmen – nicht verbindlich. Stattdessen hat das Gericht im Wege der Gesamtbetrachtung einen Ausgleich zwischen den einzelnen Stufen zugelassen, was den Mitgliedstaaten erhebliche Umsetzungsspielräume verschafft, der Rechtssicherheit aber abträglich ist. Bezogen auf gezielte, heimliche Überwachungen nimmt die Drei Stufen-Kontrolle somit im Ergebnis eine Leitbildfunktion ein. Mit Sicherheit konventionskonform ist ein Kontrollregime für heimliche und gezielte nachrichtendienstliche Maßnahmen dennoch nur, wenn es die vom EGMR formulierten Anforderungen auf den Ebenen der Genehmigung, der Durchführung und der nachträglichen Kontrolle beachtet.

b. Vorgaben für die Kontrolle von „Massenüberwachung“

Der EGMR hatte in der Vergangenheit bereits zu Systemen anlassloser Telekommunikationsüberwachung entschieden und dort hinsichtlich der Kontrolle die gleichen Maßstäbe wie bei gezielten Überwachungen angewandt⁵⁸⁸, in seinen Urteilen zu *Big Brother Watch gegen UK*⁵⁸⁹ und *Centrum för Rättvisa gg. Schweden* vom 25. Mai 2021 allerdings neue, detailliertere Maßstäbe entwickelt. Als Begründung für die Anpassung der Vorgaben führt der EGMR an, dass die technischen Entwicklungen die Kommu-

⁵⁸⁷ EGMR 18.5.2010 – 26839/05 Rn. 167 – Kennedy gg. UK.

⁵⁸⁸ EGMR 29.6.2006 – 54934/00 – Weber und Saravia gg. Deutschland; EGMR 1.7.2008 – 58243/00 – Liberty und andere gg. UK, so auch der EGMR selbst in EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 322 – Big Brother Watch gg. UK.

⁵⁸⁹ Das Urteil wird kritisiert, weil das Gericht darin die grundsätzliche Notwendigkeit der strategischen Überwachung und deren Vereinbarkeit mit Art. 8 EMRK anerkannt hat. Statt den Schwerpunkt auf die Prüfung der Legalität der Maßnahme an sich zu legen, würde der EGMR sich auf einen „prozeduralen Fetischismus“ versteifen, vgl. *Zalnieriute*, Verfassungsblog vom 2.6.2021; ähnlich Pinto de Albuquerque, EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 2. Sondervotum, Rn. 34 – Big Brother Watch gg. UK; *Watt*, Verfassungsblog vom 21.4.2022.

nikation der Menschen wesentlich verändert hätten, dass Menschen ihre Leben zunehmend online lebten und es dementsprechend mehr Daten mit einer höheren Qualität gäbe als noch vor zehn Jahren, sodass der Umfang der anlasslosen Telekommunikationsüberwachung damals kleiner war.⁵⁹⁰ Im Vergleich zur gezielten Überwachung seien die Kontrollen („supervision and review“) bei „Massenüberwachungen“ noch wichtiger, da ein inhärentes Missbrauchsrisiko bestehe und der Staat aus Gründen der nationalen Sicherheit keine Informationen zur Funktionsweise des Systems offenlege.⁵⁹¹

Wie in seiner Rechtsprechung zu individuellen Überwachungsmaßnahmen begründet der EGMR das Kontrollbedürfnis von Massenüberwachung damit, dass die durch die heimliche Vorgehensweise bedingten fehlenden Rechtsschutzmöglichkeiten kompensiert werden müssen.⁵⁹² Darüber hinaus ist auch der EGMR der Ansicht, dass die Verfahrensvorgaben (zu) weite Befugnisnormen kompensieren können.⁵⁹³

aa) Begriff der „bulk interception“

„Bulk interception“ ist nach den Ausführungen des EGMR grundsätzlich auf internationale Kommunikation ausgerichtet, schließt allerdings die Überwachung von Betroffenen innerhalb eigener Landesgrenzen nicht zwingend aus.⁵⁹⁴ Damit ist der Begriff der „bulk interception“ weiter als der der strategischen Ausland-Fernmeldeaufklärung. Die Aussagen des EGMR gelten daher auch für die strategische Fernmeldeüberwachung nach dem G 10.⁵⁹⁵

⁵⁹⁰ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 341 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 255 – Centrum för Rättvisa gg. Schweden.

⁵⁹¹ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 349 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 263 – Centrum för Rättvisa gg. Schweden.

⁵⁹² EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 336 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 250 – Centrum för Rättvisa gg. Schweden, vgl. [Teil 2 B. I. 4. a.](#)

⁵⁹³ „Consequently, in the Court’s view, a regime which permits bulk interception to be ordered on relatively wide grounds may still comply with Article 8 of the Convention, provided that, when viewed as a whole, sufficient guarantees against abuse are built into the system to compensate for this weakness.“; EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 370 – Big Brother Watch gg. UK; *Steiner*, GSZ 2024, 32, 34; kritisch hingegen das Sondervotum der Richter Lemmens, Vehabovic und Bosnjak zu EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Sondervotum Rn. 22 – Big Brother Watch gg. UK: „However, if the substantive criteria are vague, overly broad or even non-existent, the requirement of prior authorisation will necessarily fail to provide for sufficiently effective protection against arbitrariness and abuse“.

⁵⁹⁴ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 344 – Big Brother Watch gg. UK.

⁵⁹⁵ *Huber*, NVwZ-Beilage 2021, 3; *Steiner*, GSZ 2024, 32, 33.

bb) Vier Stufen der Strategischen Überwachung

Zunächst unterscheidet das Gericht vier Stufen der „Massenüberwachung“: Erstens das Abfangen der Kommunikation und der zugehörigen Verkehrsdaten, zweitens die Filterung dieser Daten anhand spezifischer Suchbegriffe (Selektoren), drittens die Analyse der auf diese Weise ausgewählten Daten und viertens die Speicherung, Nutzung und Übermittlung von Daten. Art. 8 EMRK ist stets anwendbar, wobei die Eingriffsintensität auf jeder Stufe zunimmt.⁵⁹⁶

cc) „Ende zu Ende-Schutzmechanismen“

Um das Missbrauchsrisiko zu senken, formuliert das Gericht „Ende zu Ende-Schutzmechanismen“, die es als „Eckpfeiler“ eines jeden mit Art. 8 EMRK vereinbaren Systems von „Massenüberwachungen“ zu beachten gälte: Neben der Notwendigkeit und Verhältnismäßigkeit der Maßnahme, die auf jeder der vier Stufen zu prüfen sind, zählt dazu auch die unabhängige Kontrolle in den drei bekannten Stufen (Genehmigung, Durchführung, Ex post-Kontrolle).⁵⁹⁷

dd) Ex ante-Genehmigung

Die Genehmigung, in der Objekt und Umfang der Maßnahme festgelegt werde, müsse unabhängig erteilt werden. Mit der Genehmigung ein Gericht zu betrauen, sei zwar ein „wichtiger, aber kein notwendiger Schutzmechanismus“. Stattdessen könne die Maßnahme auch von einer von der Exekutive unabhängigen Einrichtung genehmigt werden (*Kontrollleur und Modalität*).⁵⁹⁸

⁵⁹⁶ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 325 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 239 ff., 244 – Centrum för Rättvisa gg. Schweden.

⁵⁹⁷ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 350 – Big Brother Watch gg. UK: "(...) see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process"; EGMR 25.5.2021 – 35252/08 Rn. 264 – Centrum för Rättvisa gg. Schweden; vgl. auch Steiner, GSZ 2024, 32, 33 f.

⁵⁹⁸ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 351 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 265 – Centrum för Rättvisa gg. Schweden, dies kritisiert Richter Pinto de Albuquerque in seinem Sondervotum zu Big Brother Watch gg. UK (Rn. 19): "I do not see why a State governed by the rule of law should not trust its serving judges, ultimately its more senior and experienced judges, to decide on such matters. Unless the Court believes that judicial-like bodies are more independent than ordinary courts (...)" ; in seinem Sondervotum zu Rättvisa gg. Schweden kritisiert er, dass die Mitglieder des Vorabkontroll-Gremiums von der Regierung ernannt werden und wiedergewählt werden könnten, was ihre politische Bindung an die Regierung verstärke, Rn. 9.

In der Anordnung müssten der Zweck der Maßnahme sowie die für die Überwachung ausgewählten Träger elektronischer Kommunikation⁵⁹⁹ und Kommunikationsrouten genannt werden (*Kontrolltiefe*). Darüber hinaus müssen „mindestens“ die Kategorien von Selektoren, die benutzt werden sollen, bezeichnet werden. Der EGMR verdeutlicht, dass er es wegen der enormen Bedeutung der Selektorenfestlegung vorziehen würde, wenn die Selektoren in der Anordnung konkret benannt würden und dass er die Bezeichnung von Kategorien anstatt konkreter Selektoren nur akzeptiert, um den praktischen Bedürfnissen mancher Konventionsstaaten entgegenzukommen.⁶⁰⁰

Auch für die Nutzung sog. starker Selektoren (Selektoren, mit denen eine konkrete Person identifiziert werden kann, z.B. eine E-Mail-Adresse) besteht keine Pflicht zur Vorabkontrolle einzelner Selektoren, hierfür muss dann jedoch zwingend eine interne Genehmigung eingeholt werden.⁶⁰¹

Die Vorabkontrolle nach dem britischen Recht hat der EGMR im Ergebnis als nicht konventionskonform beurteilt, weil der dafür zuständige Minister als Teil der Exekutive nicht unabhängig ist, weil in der Anordnung zur Genehmigung keine Kategorien von Selektoren angegeben werden müssen und weil für starke, auf Einzelpersonen bezogene Selektoren keine interne Vorabgenehmigung erfolgen muss. Diese Mängel könnten durch die unabhängige und effektive Kontrolle auf der zweiten und dritten Stufe nicht mehr ausgeglichen werden.⁶⁰²

Demgegenüber bewertet der EGMR die Vorabkontrolle durch den schwedischen „Foreign Intelligence Court“ als konventionskonform: Der „Foreign Intelligence Court“ sei zweifellos unabhängig, weil er rechtlich bindende Entscheidungen trifft und seine Mitglieder für eine vierjährige Amtszeit von der Regierung ernannt werden. Zudem hebt der EGMR hervor, dass in der Genehmigungsanordnung die Selektoren oder

⁵⁹⁹ Albuquerque schreibt in seinem Sondervotum Big Brother Watch gg. UK, dass es sich dabei hauptsächlich um Glasfaserkabel auf dem Meeresboden handele, vgl. Rn. 3 des Sondervotums.

⁶⁰⁰ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 352 f., 354 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 266 ff. – Centrum för Rättvisa gg. Schweden; vgl. auch *Steiner*, GSZ 2024, 32, 36; Albuquerque hingegen schreibt in Rn. 20 seines Sondervotums zu Big Brother Watch gg. UK, dass die Selektoren konkret benannt werden müssten. Huber weist darauf hin, dass der G 10-Kommission alle Suchbegriffe in den entsprechenden Anträgen ausführlich erläutert würden und er in Anbetracht des deutschen Beispiels das Argument mancher Regierungen, die Effektivität der Maßnahme würde durch Nennung von Selektoren leiden, nicht nachvollziehen kann, *Huber*, NVwZ-Beilage 2021, 3, 5.

⁶⁰¹ Nachdem der EGMR feststellt, dass aus praktischen Bedürfnissen auf die Nennung der einzelnen Selektoren verzichtet werden kann, fordert er zumindest „enhanced safeguards“ für die Nutzung starker Selektoren, EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 355 – Big Brother Watch gg. UK; vgl. auch *Steiner*, GSZ 2024, 32, 36.

⁶⁰² EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 425, 377 ff. – Big Brother Watch.

zumindest Kategorien von Selektoren bezeichnet werden müssen. Der „Foreign Intelligence Court“ kontrolliere umfassend, weil der Kontrollgegenstand das Ziel der Datenerhebung, die Kommunikationsträger und die Kategorien von Selektoren umfasse.⁶⁰³

ee) Kontrolle während der Durchführung

Während der Durchführung der Maßnahme solle jede Stufe der Massenüberwachung⁶⁰⁴ inklusive des unabhängigen Genehmigungsprozesses und möglicher Entscheidungen über eine Erneuerung der Genehmigung, die Löschung der Daten und Datenübermittlungen von Staaten, die keine Konventionsstaaten sind, kontrolliert werden (*Kontrolltiefe*). Dafür sei eine unabhängige Einrichtung zuständig, die „ausreichend widerstandsfähig“ (im Original: „sufficiently robust“) sein soll, um den Eingriff im Rahmen dessen zu halten, was in einer demokratischen Gesellschaft notwendig ist (*Distanz*). Vor allem müsse der Kontrolleur in der Lage sein, die Notwendigkeit und Verhältnismäßigkeit einzuschätzen, weshalb die Nachrichtendienste auf jeder der vier Stufen detaillierte Aufzeichnungen machen sollen.⁶⁰⁵

Damit ist evident, dass der Kontrolleur Zugang zu den Aufzeichnungen haben soll (*Kontrollmittel zur Informationsgewinnung*).

Ob mit der Formulierung „ausreichend widerstandsfähig“ gemeint ist, dass der Kontrolleur mit wirksamen Befugnissen und bzw. oder Ressourcen oder Kontrollergebnisfolgen ausgestattet werden muss, ist offen, was den Gestaltungsspielraum der Konventionsstaaten erhöht.⁶⁰⁶

Der EGMR schweigt zur Häufigkeit der Kontrollen (*Modalität*), in einem Sondervotum wird jedoch gefordert, die Durchführung regelmäßig, in „ausreichend kurzen Intervallen“, zu kontrollieren.⁶⁰⁷

Die britische und schwedische Aufsicht hat der EGMR als konventionskonform eingeordnet.

⁶⁰³ EGMR 25.5.2021 – 35252/08 Rn. 296 ff. – Centrum för Rättvisa gg. Schweden.

⁶⁰⁴ Vgl. [Teil 2 B. I. 4. a.](#)

⁶⁰⁵ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 356, 499 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 270 – Centrum för Rättvisa gg. Schweden.

⁶⁰⁶ Albuquerque fordert in EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Sondervotum Rn. 29 – Big Brother Watch gg. UK außerdem: “Last but not least, human and financial oversight resources and capabilities should match the scale of the operations being overseen, otherwise the entire system will be a mere façade covering the discretionary administrative process of the intercepting authorities”.

⁶⁰⁷ Albuquerque, EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Sondervotum Rn. 34 – Big Brother Watch gg. UK.

Den in Großbritannien bis 2017⁶⁰⁸ für die Aufsicht der Kommunikationsverarbeitung zuständigen „Interception of Communications Commissioner“ (IC Commissioner), ein (ehemaliger) hoher Richter, der vom Premierminister ernannt wird, erachtet der EGMR – ohne nähere Begründung – als unabhängig.⁶⁰⁹

Um seine Kontrollfunktion wahrnehmen zu können, hatte der IC Commissioner das Recht, alle gewünschten Informationen zu erhalten und Dokumente einzusehen, während die Nachrichtendienste gesetzlich verpflichtet waren, jede Stufe der Massenüberwachung zu protokollieren. Seine Kontrolle erstreckte sich auch auf die Wahl der Selektoren und Kommunikationsträger. Wenn er Empfehlungen an die Behördenleitung richtete, musste diese innerhalb von zwei Monaten darauf antworten und darlegen, welche Maßnahmen sie ergriffen hatte. Der IC Commissioner erstattete dem Premierminister halbjährlich, dem Parlament jährlich Bericht über seine Ergebnisse. Seine Kontrollberichte wurden sogar veröffentlicht.⁶¹⁰

Das für die Aufsicht in Schweden hauptsächlich zuständige⁶¹¹ „Foreign Intelligence Inspectorate“ sei unabhängig, weil es aus (ehemaligen) Richtern zusammengesetzt ist, die vom Parlament vorgeschlagen und von der Regierung für vier Jahre ernannt werden. Das „Foreign Intelligence Inspectorate“ verfüge über „weitreichende Befugnisse“, um den gesamten Prozess der strategischen Überwachung zu kontrollieren. Als eine solche weitreichende Befugnis nennt der EGMR, dass das Inspectorate über den Zugang der Nachrichtendienste auf die Träger der elektronischen Kommunikation entscheidet, indem er den beantragten Zugang mit der Genehmigung abgleicht. Der EGMR hebt außerdem hervor, dass das Inspectorate jeden Verarbeitungsschritt kontrolliert, Zugang zu allen relevanten Dokumenten hat und die genutzten Selektoren überprüft.⁶¹²

⁶⁰⁸ Nach einer Gesetzesänderung ist seit 2017 stattdessen das „Investigatory Powers Commissioners Office“ zuständig, EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 138 – Big Brother Watch. Die Entscheidung hingegen bezieht sich auf Klagen aus den Jahren 2013, 2014 und 2014, vgl. Rn. 1.

⁶⁰⁹ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 407 – Big Brother Watch sowie die vorangehende Kammerentscheidung v. 13.9.2018 – 58170/13, 62322/14, 24960/15 Rn. 378; zur Ernennung vgl. Section 57 para 1 Regulation of Investigatory Powers Act 2000.

⁶¹⁰ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 407, 412 – Big Brother Watch sowie die vorangehende Kammerentscheidung v. 13.9.2018 – 58170/13, 62322/14, 24960/15 Rn. 378.

⁶¹¹ Daneben sei auch der Datenschutzbeauftragte für die Kontrolle auf der zweiten Stufe zuständig, der jedoch im Vergleich über geringere Kompetenzen verfüge, EGMR 25.5.2021 – 35252/08 Rn. 345 – Centrum för Rättvisa gg. Schweden.

⁶¹² EGMR 25.5.2021 – 35252/08 Rn. 346 ff. – Centrum för Rättvisa gg. Schweden.

ff) Ex post-Kontrolle

Nach Beendigung der Maßnahme (auf der dritten Stufe) soll ein Gericht oder eine von der Exekutive unabhängige Institution kontrollieren (*Kontrolleur und Distanz*). Nach einer Benachrichtigung können Betroffene den Rechtsbehelf initiieren. Soweit keine Benachrichtigung vorgesehen ist, müsse ein alternativer Rechtsbehelf etabliert werden, der vom Nachweis tatsächlicher Betroffenheit unabhängig ist. Der EGMR betont, dass solche Rechtsbehelfe „effektiv“ sind und gegebenenfalls sogar bessere Garantien für ein ordentliches Verfahren böten als Rechtsbehelfe, die von einer Benachrichtigung abhängig sind, da zum Schutz der nationalen Sicherheit womöglich weitgehende Ausnahmen von der Benachrichtigungspflicht existieren oder der Aufenthaltsort des Betroffenen nicht identifiziert werden kann. Gegenstand der Beschwerde könne entweder die konkrete Maßnahme oder die Konventionsvereinbarkeit des Überwachungsregimes generell sein. Außerdem soll sich die Kontrolle auf Datenübermittlungen durch Nicht-Konventionsstaaten erstrecken.⁶¹³

Wenn für die Kontrolle während der Durchführung und nach der Beendigung derselbe Kontrolleur zuständig ist, besteht die Gefahr von Interessenskonflikten, da der Kontrolleur sein eigenes Vorgehen auf der zweiten Stufe beurteilen muss. Daher muss grundsätzlich auf jeder Stufe ein anderer Kontrolleur vorgesehen werden. Sollte nur eine Institution mit der Kontrolle auf zwei Stufen beauftragt sein, kann dies noch konventionskonform sein, wenn diese Kontrolle ihrerseits durch eine andere Behörde beaufsichtigt wird.⁶¹⁴

Der EGMR betont, dass die Befugnisse und prozeduralen Garantien für die Beurteilung der Effektivität eines Rechtsbehelfs entscheidend sind. Wenn möglich, solle das Verfahren kontradiktorisch erfolgen. Die Entscheidungen des Kontrolleurs sollen begründet und unter anderem bezogen auf die Beendigung einer rechtswidrigen Maßnahme und die Löschung rechtswidrig erlangten Materials rechtlich bindend sein (*Kontrollergebnisfolgen*). Außerdem erachtet der EGMR die Veröffentlichung der begründeten Entscheidung als sinnvoll.⁶¹⁵

Die ex post-Kontrolle durch das britische „Investigatory Powers Tribunal“ (IPT), dessen Mitglieder vorher entweder an einem hohen Gericht oder mindestens zehn Jahre als Anwalt gearbeitet haben müssen und bei dem der Vorsitz von einem „High Court Judge“ ausgeübt werden muss, bewertet der EGMR als konventionskonform. Der EGMR hebt hervor, dass das IPT umfassend zuständig ist, dass Betroffene sich ohne

⁶¹³ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 357 f, 499 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 271 ff. – Centrum för Rättvisa gg. Schweden.

⁶¹⁴ EGMR 25.5.2021 – 35252/08 Rn. 359, 360, 364 – Centrum för Rättvisa gg. Schweden; dies ebenfalls ansprechend *Steiner*, GSZ 2024, 32, 37.

⁶¹⁵ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 359 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 273, 361 – Centrum för Rättvisa gg. Schweden; *Steiner*, GSZ 2024, 32, 37.

Nachweis einer tatsächlichen Betroffenheit und Benachrichtigung an ihn wenden können und gegenüber dem IPT alle notwendigen Dokumente offengelegt werden müssen. Das IPT verhandelt – wenn möglich – in offenen Anhörungen, in geschlossenen Verhandlungsterminen kann es den „Counsel to the Tribunal“ bitten, die Klägerseite an Stelle der Betroffenen zu repräsentieren. Wenn das IPT einen Verstoß feststellt, kann es frei entscheiden, wie es reagiert und dem Betroffenen beispielsweise Schadensersatz zusprechen oder die Anordnung aufheben und die Löschung personenbezogener Daten anordnen.⁶¹⁶

Im Gegensatz dazu hat der EGMR entschieden, dass die schwedische Rechtslage konventionswidrig ist. Zwar haben Betroffene auch dort das Recht, einen nachträglichen Rechtsbehelf zu erheben ohne dafür eine tatsächliche Betroffenheit geltend machen zu müssen. Dass diese Beschwerde allerdings an das „Foreign Intelligence Inspectorate“ zu richten ist, das zugleich für die Kontrollen auf der zweiten Stufe zuständig ist und in dieser Funktion auch den Zugang zu den Signalträgern mitverantwortet, erachtet der EGMR wegen potenzieller Interessenskonflikte als problematisch. Dieser Nachteil könne nicht dadurch ausgeglichen werden, dass das „Foreign Intelligence Inspectorate“ grundsätzlich selbst durch eine andere Institution kontrolliert wird, weil gesetzlich nicht geregelt ist, dass diese Kontrollen (regelmäßig) erfolgen. Darüber hinaus kritisiert der EGMR, dass die Entscheidungen, die das „Foreign Intelligence Inspectorate“ auf Betroffenenbeschwerden hin trifft, nicht begründet werden müssen – weder gegenüber dem Betroffenen noch gegenüber einem sicherheitsüberprüften Spezialanwalt. Ein solches System sei nach Auffassung des EGMR zu abhängig von der „Initiative und Beharrlichkeit“ gewählter Beamter, die abseits der Öffentlichkeit agieren.⁶¹⁷

gg) Verbindlichkeit der Vorgaben

Die oben beschriebenen Schutzmechanismen zur Kontrolle von anlassloser Telekommunikationsüberwachung betreffen nur drei der insgesamt acht Kriterien, die der EGMR formuliert hat (Kriterium 3, 7, 8). Insgesamt muss die gesetzliche Grundlage nach der Rechtsprechung des EGMR festlegen:

- aus welchen Gründen die bulk interception erfolgen kann (1. Kriterium),
- unter welchen Umständen sie zulässig ist (2. Kriterium),
- dass ein Genehmigungsverfahren vorgesehen ist (3. Kriterium),
- welche Regeln für die Verarbeitung der Daten gelten (4. Kriterium),
- welche Vorkehrungen bei Übermittlungen an Dritte zu beachten sind (5. Kriterium),

⁶¹⁶ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 413-415 – Big Brother Watch gg. UK.

⁶¹⁷ EGMR 25.5.2021 – 35252/08 Rn. 354 ff. – Centrum för Rättvisa gg. Schweden.

- wie lange die Daten verarbeitet werden dürfen und wann sie zu löschen sind (6. Kriterium),
 - welche Verfahren und Modalitäten für die Aufsicht durch eine unabhängige Einrichtung gelten, die prüft, ob die anderen Schutzmechanismen eingehalten werden und Verstöße ahnden kann (7. Kriterium),
 - welche Verfahren für unabhängige Ex-post-Kontrollen der Vereinbarkeit etabliert sind und welche Befugnisse der Kontrolleur hat, Verstöße zu ahnden (8. Kriterium).⁶¹⁸
- Ob diese acht Kriterien des EGMR für die Ausgestaltung einer konventionskonformen anlasslosen Überwachung von Telekommunikation verbindlich sind, ist unklar.⁶¹⁹ Der Grund für die Unsicherheit ist folgende Urteils Passage: „In the light of the above, the Court will determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime“⁶²⁰. Die „Gesamt Betrachtung“ des Gerichts deute darauf hin, dass eine Abwägung zwischen unterschiedlichen Schutzmechanismen möglich wäre.⁶²¹ Drei Richter des EGMR schreiben dazu in einem Sondervotum:

*„We would add that an approach setting minimum standards as absolute limits, as thick red lines that may not be crossed, would provide for a stricter and more foreseeable protection, which is of utmost importance in a field where the action of the State authorities is conducted with a high level of secrecy (...)“*⁶²²

Da nicht vorhersehbar ist, wie die Gesamtbetrachtung des EGMR im Einzelfall ausfallen würde, ist es rechtssicherer, alle acht Kriterien umzusetzen, wenn eine konventionskonforme Regelung angestrebt wird.

⁶¹⁸ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 361 – Big Brother Watch gg. UK.; EGMR 25.5.2021 – 35252/08 Rn. 275 – Centrum för Rättvisa gg. Schweden; *Steiner*, GSZ 2024, 32, 34.

⁶¹⁹ *Zalnieriute*, Verfassungsblog vom 2.6.2021: „Are these criteria mandatory and cumulative, or semi-optional? Unfortunately, the GC [Grand Chamber] is silent on this point“.

⁶²⁰ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 360 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 274 – Centrum för Rättvisa gg. Schweden.

⁶²¹ Richter Lemmens, Vehabovic, Bosnjak in EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Sondervotum Rn. 14 f. – Big Brother Watch gg. UK: „However, the criteria included in this list: (a) do not clearly serve as self-standing minimum standards, as any lack of compliance with any of those standards appears to be ‘reparable’ in the process of a global assessment“; ebenso Albuquerque in EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Sondervotum Rn. 15 – Big Brother Watch gg. UK, der in scharfem Ton warnt: „In some corners of Europe, zealous secret services will be strongly tempted to take advantage of the Court’s very lax fashion of formulating legal standards and innocent people will pay the price sooner or later“.

⁶²² Richter Lemmens, Vehabovic, Bosnjak, in EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Sondervotum Rn. 15 – Big Brother Watch gg. UK.

Zudem hat der EGMR betont, dass gerade die drei Kontrollstufen (Kriterium 3, 7, 8) als „Eckpfeiler“ einer konventionskonformen Ausgestaltung stets zu beachten seien.⁶²³ Dafür spricht auch, dass die Mängel bei der Vorabkontrolle nach der englischen Rechtslage und die Mängel bei der ex post-Kontrolle im schwedischen Recht nicht ausgeglichen werden konnten und der EGMR in beiden Fällen eine Verletzung von Art. 8 EMRK bejaht hat.⁶²⁴

c. Relevanz der Eingriffsintensität

Im Folgenden soll beantwortet werden, inwieweit die Eingriffsintensität der Maßnahme Auswirkungen auf diese Anforderungen hat.

Ob Kontrollen notwendig sind, macht der EGMR grundsätzlich nicht so eindeutig wie das Bundesverfassungsgericht von der (hohen) Eingriffsintensität der Maßnahmen abhängig. Stattdessen begründet er seine Vorgaben an die Kontrolle heimlicher, zielgerichteter Maßnahmen damit, dass beim Einsatz dieser nachrichtendienstlichen Mittel hohe Missbrauchsrisiken bestehen.⁶²⁵

aa) Eindeutige Relevanz für die Kontrolle der Massenüberwachung

In den neuesten Urteilen zur strategischen Überwachung wird jedoch unter anderem explizit die steigende Eingriffsintensität auf den vier Stufen („increasing degrees of intrusion“) der Massenüberwachung als Begründung dafür genannt, weshalb die Sicherungsmechanismen im Vergleich zur gezielten Überwachung verschärft werden mussten.⁶²⁶

⁶²³ Vgl. [Teil 2 B. I. 4. b. cc](#)); andere Ansicht *Zalnierute*, American Journal of International Law 2022, 585, 590: „But it is not clear if any of the requirements are mandatory. It rather seems that non-compliance with one or several is not fatal“; ähnlich wohl *Winter*, Kohärenz des Nachrichtendienstrechts, S. 323, die sich allerdings nicht auf die Entscheidung der Großen Kammer aus 2021 bezieht.

⁶²⁴ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 425 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 372 f. – Centrum för Rättvisa gg. Schweden.

⁶²⁵ „(...) [I]n a field where abuse is potentially so easy in individual cases“, EGMR 6.9.1978 – 5029/71 Rn. 56 – Klass und andere gg. Deutschland; EGMR 18.5.2010 – 26839/05 Rn. 167 – Kennedy gg. UK; vgl. auch, „...risk of abuse inherent in any system of secret surveillance“, EGMR 28.6.2007 – 62540/00 Rn. 93 – Assoc. For European Integration and Human Rights and Ekimdzhiiev gg. Bulgarien.

⁶²⁶ Vgl. [Teil 2 B. I. 4. b.](#); die Eingriffsintensität der strategischen Überwachung ist immer hoch, weshalb der EGMR hier detailliertere Vorgaben an das Kontrolldesign formuliert hat. Während die Eingriffsintensität mit jeder Stufe der Massenüberwachung steigt (EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 347 – Big Brother Watch gg. UK; EGMR 25.5.2021 – 35252/08 Rn. 261 – Centrum för Rättvisa gg. Schweden), bleiben die Anforderungen an die Kontrolle gleich streng.

bb) Geringere Bedeutung für gezielte Überwachung

In den zitierten, bekannteren Entscheidungen des EGMR über gezielte nachrichtendienstliche Überwachungsmaßnahmen ist in den Urteilspassagen über die Kontrollanforderungen kein Bezug zur Eingriffsintensität erkennbar. Stattdessen werden manche Aspekte, die für die Festlegung der Eingriffsintensität nach deutschem Verfassungsrecht ausschlaggebend sind, lediglich vorab als relevante Faktoren für die Verhältnismäßigkeitsabwägung beschrieben („nature, scope and duration of the possible measures“).⁶²⁷

In diesem Zusammenhang hat der EGMR in der aktuellen Entscheidung *Ekimdzhiyev und andere gg. Bulgarien* klargestellt, dass die Vorgaben, die für die Prüfung der Vereinbarkeit von „geheimen Überwachungsmaßnahmen, inklusive der Kommunikationsüberwachung“ mit Art. 8 Abs. 2 EMRK gelten, in der Entscheidung *Zakharov gg. Bulgarien* „detailliert“ beschrieben worden seien. Es sei nicht notwendig, alle dieser Prinzipien zu wiederholen, aber es müsse betont werden, dass ein System geheimer Überwachungen effektive Garantien enthalten muss, „vor allem Nachprüfungs- und Aufsichtsarrangements (...)“.⁶²⁸

Dass der EGMR in dieser Entscheidung und auch zuvor⁶²⁹ im Kontext der Kontrolle nur von „geheimen Überwachungsmaßnahmen“ spricht, für die die Anforderungen gelten, ohne nach konkreten Befugnissen zu differenzieren, kann so interpretiert werden, dass die Anforderungen für alle geheimen Überwachungsmaßnahmen gleich sind und es daher für das Kontrolldesign einzelner Maßnahmen nicht auf die Eingriffsintensität ankommt.

Andererseits hat der EGMR bei anderen Befugnissen teilweise auf deren geringere Eingriffsintensität abgestellt und niedrigere Kontrollanforderungen formuliert. In der Entscheidung *Breyer gg. Deutschland* beispielsweise, in der es um die Konventionskonformität der Bevorratungspflicht und Abrufmöglichkeit von Bestandsdaten ging, ist der EMRK zwar auf die drei Stufen der Kontrolle eingegangen, schreibt aber relativierend, dass der Umfang der Kontrolle hier „ein wichtiges, aber nicht entscheidendes Element“ für die Beurteilung der Verhältnismäßigkeit darstelle. Er begründet dies damit, dass es sich beim Datenzugang zu Bestandsdaten – anders als beispielsweise bei den u.a. in *Roman Zakharov gg. Russland* zu prüfenden Befugnissen – um „keinen individualisierten und keinen so intensiven Eingriff“ in Art. 8 EMRK handele.⁶³⁰

⁶²⁷ EGMR 4.12.2015 – 47143/06 Rn. 232 – *Roman Zakharov gg. Russland*; EGMR 2.1.2016 – 37138/14, Rn. 57 – *Szabó und Vissy gg. Ungarn*.

⁶²⁸ EGMR 11.4.2022 – 70078/12 Rn. 291 f. – *Ekimdzhiyev und andere gg. Bulgarien*.

⁶²⁹ EGMR 4.12.2015 – 47143/06 Rn. 233 – *Roman Zakharov gg. Russland*; EGMR 28.6.2007 – 62540/00 Rn. 77 – *Assoc. For European Integration and Human Rights and Ekimdzhiyev gg. Bulgarien*.

⁶³⁰ EGMR 30.1.2020 – 50001/12 Rn. 103 – *Breyer gg. Deutschland*.

Auf die Abrufmöglichkeiten der deutschen Nachrichtendienste geht der EGMR in *Breyer gg. Deutschland* nicht ein. Trotz der niedrigeren Eingriffsintensität, die eine geringere Bedeutung der Kontrollmechanismen in der Verhältnismäßigkeitsabwägung zur Folge hat („wichtiges, aber nicht entscheidendes Element“), prüft der EGMR die Kontrolle und resümiert, dass „die Möglichkeit der Kontrolle durch die zuständigen Datenschutzbehörden eine Überprüfung durch eine unabhängige Stelle gewährleistet“ und jeder gegenüber den Datenschutzbeauftragten von Bund und Ländern einen Rechtsbehelf erheben könne.⁶³¹ Der EMRK prüft also die zweite und dritte Kontrollstufe und wendet damit die drei Stufen-Kontrolle an, obwohl die Bedeutung des Kontrolldesigns innerhalb der Verhältnismäßigkeitsprüfung bei Maßnahmen mit geringerer Eingriffsintensität sinkt. Dass das Fehlen einer unabhängigen Genehmigung im Rahmen einer Gesamtbetrachtung durch Vorkehrungen auf der zweiten und dritten Stufe ausgeglichen werden kann, war bereits zuvor bekannt.

In einer anderen Entscheidung, in der der EGMR geringere Kontrollanforderungen mit einer geringeren Eingriffsintensität begründet hat, ging es um die Konventionskonformität einer strafprozessualen Erlaubnis zur technikgestützten Observation. Der EGMR argumentierte, dass die GPS-Überwachung im öffentlichen Raum weniger eingriffsintensiv ist als Telekommunikationsüberwachungen, was sich auf die Verhältnismäßigkeitsanforderungen auswirke: eine Vorabkontrolle sei nicht erforderlich, die nachträgliche Kontrolle durch ein Gericht ausreichend.⁶³²

Während der EGMR in seinen bekannteren Entscheidungen zum Nachrichtendienstrecht in Bezug auf die Kontrollen nicht auf die Eingriffsintensität eingeht, sondern für geheime Überwachungsmaßnahmen generelle Anforderungen formuliert, hat die Eingriffsintensität in anderen Entscheidungen Folgen für die Kontrollanforderungen. Im Ergebnis wirkt sich die Differenzierung nach der Eingriffsintensität bei gezielten Maßnahmen aber ohnehin kaum aus, weil die drei Stufen auch bei eingriffsintensiven Maßnahmen nicht strikt gelten, sondern einander in einer Gesamtbetrachtung ausgleichen können⁶³³.

⁶³¹ EGMR 30.1.2020 – 50001/12 Rn. 105 ff. – Breyer gg. Deutschland.

⁶³² EGMR 2.12.2010 – 35623/05 Rn. 72 – Uzun gg. Deutschland.

⁶³³ Vgl. [Teil 2 B. I. 4. a. dd.](#)

II. Unionsrechtliche Vorgaben

„These rulings [Cases of Privacy International and Quadrature du net] suggest that the CJEU has become an important actor in the national security landscape, which has traditionally been outside the scope of the European integration (...)“

Monika Zalnieriute⁶³⁴

Bisher gab es im Nachrichtendienstrecht keine unionsrechtliche Dimension.⁶³⁵ Mit der neueren Rechtsprechung des EuGH hat sich das jedoch geändert (vgl. 1.). Bestimmte Aufgaben der Nachrichtendienste sind seitdem unter europäisches Sekundärrecht subsumierbar, was Auswirkungen auf die Rechtskontrolle (vgl. 2.) und die Anwendbarkeit von Unionsgrundrechten (vgl. 3.) hat.

1. Anwendungsbereich des Unionsrechts: Ausnahme zur „nationalen Sicherheit“

Zwei Regelungswerke des Unionsrechts würden die Rechtskontrolle der Nachrichtendienste maßgeblich beeinflussen, wenn sie anwendbar wären: die DSGVO (VO 2016/679) und die JIRL (RL 2016/680). Beide Gesetze gelten allerdings nur, soweit die Datenverarbeitung der Nachrichtendienste „in den Anwendungsbereich des Unionsrechts fällt“. ⁶³⁶ Diese Einschränkung ist auf die primärrechtliche Kompetenzgrundlage dieser Gesetze zurückzuführen, denn gem. Art. 16 Abs. 2 AEUV darf der Unionsgesetzgeber die Datenverarbeitungen der Mitgliedsstaaten nur regeln, wenn sie in den Anwendungsbereich des Unionsrechts fallen.

Wann der Anwendungsbereich des Unionsrechts eröffnet ist, ergibt sich aus Art. 4 EUV. Gem. Art. 4 Abs. 2 S. 2 EUV „achtet“ die Union die grundlegenden Funktionen des Staates, unter anderem „den Schutz der nationalen Sicherheit“. Art. 4 Abs. 2 S. 3 EUV legt fest, dass „die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten“ fällt. Für diese Regelungsmaterie sind somit die Mitgliedstaaten zuständig.⁶³⁷ Folglich ist der Begriff der „nationalen Sicherheit“ von zentraler Bedeutung: Nur soweit eine Materie nicht darunter subsumiert werden kann, sind die DSGVO und die JIRL anwendbar.

⁶³⁴ Zalnieriute, Modern Law Review 2022, 198, 199; ähnlich schon Cameron, International Journal of Intelligence and Counterintelligence 2020, 452, 460: „For security and intelligence agencies the CJEU is a new, and presumably unwelcome, actor that has appeared on the scene“.

⁶³⁵ Vgl. Sule, National Security, 335 Rn. 3.

⁶³⁶ Art. 2 Abs. 2 lit. a) DSGVO; Art. 3 Abs. 2 lit. a) JIRL.

⁶³⁷ Art. 4 Abs. 2 S. 3 EUV ist eine „Kompetenzausübungsschranke“ der Europäischen Union, Schwarze/Becker/Hatje/Schoo/Hatje, Art. 4 Rn. 20, ähnlich Cameron, Oversight of Intelligence Agencies

a. Definition der „nationalen Sicherheit“ in der Literatur

Lange war unklar, wie der Begriff der „nationalen Sicherheit“ auszulegen ist. Eine europaweit angewandte, allgemeingültige Definition existierte nicht.⁶³⁸ Einige plädieren dafür, den Begriff eng auszulegen: erfasst sei nur das „fundamentale Bestandsinteresse des Staates“, also „existenzielle Sicherheitsbelange“ der Mitgliedstaaten.⁶³⁹ Viele sind (teilweise nicht weiter ausdifferenzierend und begründend) der Meinung, dass die Datenverarbeitungen durch Nachrichtendienste generell unter die „nationale Sicherheit“ subsumierbar sind und damit nicht in den Anwendungsbereich des Unionsrechts fallen.⁶⁴⁰ Auch der Gesetzgeber folgt dieser Auffassung.⁶⁴¹ Das Bundesverfassungsgericht hat dies im Urteil zur strategischen Auslands-Fernmeldeaufklärung differenzierter beurteilt und festgestellt, dass der Anwendungsbereich des Unionsrechts „jedenfalls im Hinblick auf Teile des Aufgabenprofils des BND ausgeschlossen sein könnte“, „ob und inwieweit dies der Fall ist, [sei] unionsrechtlich noch nicht geklärt“.⁶⁴²

2016, 71, 93 bzw. ein „mitgliedstaatlicher Zuständigkeitsvorbehalt“, vgl. Groeben/Schwarze/Hatje/Obwexer, Art. 4 EUV Rn. 46, *Karpenstein/Sangi*, GSZ 2020, 162, 165; *Banzhaf*, Präventionsbehörden, S. 32; „mitgliedstaatlicher Prärogativbereich“ bei Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9b. Im Gegensatz dazu ergäbe sich aus der neuesten Rechtsprechung des EuGH, dass dieser Art. 4 Abs. 2 S. 3 EUV als Rechtfertigungsgrund für schwere Grundrechtseingriffe interpretiere, nicht als Zuständigkeitsvorbehalt, *Baumgartner*, GSZ 2021, 42, 44.

⁶³⁸ *Sule*, National Security, 335, 343 Rn. 23, 348 Rn. 39 ff.; für Begriffe des Unionsrechts gilt, dass sie autonom europarechtlich auszulegen sind, *Karpenstein/Sangi*, GSZ 2020, 162, 166 f.

⁶³⁹ Darauf sei der Begriff „ganz überwiegend“ begrenzt worden, vgl. vertiefend *Peuker*, EuR 2023, 535, 547; Groeben/Schwarze/Hatje/Obwexer, Art. 4 EUV Rn. 45; Schwarze/Becker/Hatje/Schoo/Hatje, Art. 4 EUV Rn. 19; mit ausführlicher Begründung insb. *Karpenstein/Sangi*, GSZ 2020, 162, 166; „Sicherheit des Staates“ bei *Botta*, CR 2020, 82, 85 Rn. 25, *Callies/Ruffert/Callies*, Art. 4 EUV Rn. 48, *Grabitz/Hilf/Nettesheim/Schill/Krenn*, Art. 4 EUV Rn. 42.

⁶⁴⁰ *Ehmann/Selmayr/Zerdick*, Art. 2 DSGVO, Rn. 8; Wolff/Brink/Wolff, § 45 BDSG Rn. 20; *Banzhaf*, Präventionsbehörden 2021, S. 33; *Johannes/Weinhold*, Datenschutzrecht bei Polizei und Justiz, S. 33 Rn. 19; *Kugelman*, DuD 2012, 581, 582; Taeger/Gabel/Schmidt, Art. 2 DSGVO Rn. 14; *Stoklas/Wendorf*, ZD-Aktuell 2016, 5345; *Schenke/Graulich/Ruthig/Schenke/Graulich/Ruthig*, Einführung S. 7 Rn. 23, etwas differenzierter *Möstl/Schwabenbauer/Schröder*, Datenschutz-Richtlinie (EU) 2016/680 (JI-RL) Rn. 15: „Jedenfalls die Bereiche Verteidigung und Auslandsnachrichtendienst dürften außerhalb des Anwendungsbereichs der Union liegen“; mit ausführlicher Herleitung des Begriffs der nationalen Sicherheit, *Karpenstein/Sangi*, GSZ 2020, 162, 167; *Rüß*, Hdb. des Rechts der Nachrichtendienste, 458, 460 f.7; a. A. Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9d; ohne nähere Begründung schon *Johannes/Weinhold*, Datenschutzrecht bei Polizei und Justiz 2018, Rn. 386, was allerdings im Widerspruch zu den Aussagen in Rn. 20 desselben Buchs steht.

⁶⁴¹ Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9 d.

⁶⁴² BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 65.

b. Definition der „nationalen Sicherheit“ durch den EuGH

Es gibt Rechtsprechung (mit Bezug zum Nachrichtendienstrecht), in der sich der EuGH zur nationalen Sicherheit geäußert hat. Das betrifft zunächst die nationale Sicherheit von Drittstaaten.⁶⁴³ Hier ist Art. 4 Abs. 2 S. 3 EUV jedoch ohnehin nicht anwendbar, da die nationale Sicherheit Dritter vom Anwendungsbereich der Norm unstrittig nicht erfasst ist.⁶⁴⁴

Darüber hinaus hat der EuGH sich im Zusammenhang mit der Verpflichtung Privater, Daten auf Vorrat zu speichern und diese an öffentliche Stellen zu übermitteln, zur „nationalen Sicherheit“ geäußert.⁶⁴⁵ In der Rechtssache *Privacy International* hatte der Gerichtshof über die Auslegung von Art. 1 Abs. 3 i. V. m. Art. 15 Abs. 1 der RL (EU) 2002/58 (ePrivacy-Richtlinie) zu entscheiden. Gemäß dieser Norm können Mitgliedsstaaten bestimmte Vorgaben dieser Richtlinie durch eigenes Recht beschränken und beispielsweise die Aufbewahrung von Daten „während einer begrenzten Zeit anordnen“, wenn dies unter anderem „für die nationale Sicherheit (...) notwendig, angemessen und verhältnismäßig“ ist. Der EuGH hat entschieden, dass sich der Staat nur auf diese Ausnahme von den Vorgaben der Richtlinie berufen kann, wenn er die Daten selbst erhebt. Übermittlungen von Verkehrs- und Standortdaten durch Private an die Sicherheitsbehörden fallen hingegen auch dann in den Anwendungsbereich der Richtlinie, wenn sie zum Schutz der nationalen Sicherheit erfolgen.⁶⁴⁶

Soweit die „nationale Sicherheit“ in europäischem Sekundärrecht als Ausnahmeklausel für die Anwendbarkeit bestimmter Vorgaben normiert ist (wie in Art. 15 Abs. 1 RL (EU) 2002/58), ist der EuGH kraft seiner Zuständigkeit für die Auslegung des Sekundärrechts auch für die Interpretation dieser Ausnahmeklauseln zuständig.⁶⁴⁷

Der EuGH hatte die nationale Sicherheit in einer Entscheidung aus 2008 mit der „Sicherheit des Staates“ gleichgesetzt.⁶⁴⁸ Im Zusammenhang mit der Prüfung von Art. 2 Abs. 2 lit.a) DSGVO, der vorsieht, dass die DSGVO auf Datenverarbeitungen im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt, nicht

⁶⁴³ EuGH C-311/18, Urteil v. 16.7. 2020 Schrems II.

⁶⁴⁴ EuGH C-311/18, Urteil v. 16.7.2020 Schrems II, Rn. 81.

⁶⁴⁵ EuGH C-623/17 v. 6.10.2020 *Privacy International*; EuGH C-511/18, C-512/18, C-520/18 v. 6.10.2020 *La Quadrature du Net*; EuGH, C-140/20 v. 5.4.2022 G.D.; EuGH C-793/19, C-794/19 v. 20.9.2022 *SpaceNet* und andere.

⁶⁴⁶ EuGH C-623/17 v. 6.10.2020 *Privacy International*, Rn. 46 ff.; Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9c; kritisch Baumgartner, GSZ 2021, 42, 43 f.

⁶⁴⁷ Vgl. Crespi, *European Law Review* 2018, 669, 676 f., wonach Unionsrecht anwendbar ist, wenn nationale Maßnahmen im Anwendungsbereich der nationalen Sicherheit mit angrenzenden, durch Unionsrecht regulierten Sachmaterien in Konflikt geraten; Anderson, *A question of trust* 2015, S. 71. Art. 4 Abs. 2 S. 3 EUV ist somit in erster Linie für den Gesetzgeber bedeutend, Cameron, *International Journal of Intelligence and Counterintelligence* 2020, 452, 459.

⁶⁴⁸ EuGH C-275/06 v. 29.1.2008 *Promiscuae*, Rn. 49.

anwendbar ist, entschied der EUGH 2021, dass Tätigkeiten, die der nationalen Sicherheit dienen, „den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft bezwecken“.⁶⁴⁹ In seinen Entscheidungen zu den Rechtssachen *La Quadrature du Net und andere* sowie *Privacy International* vom 6. Oktober 2020 hat das Gericht den Begriff erstmals ausführlich definiert:

*„Insoweit ist zunächst festzustellen, dass nach Art. 4 Abs. 2 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Diese Verantwortung entspricht dem zentralen Anliegen, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten.“*⁶⁵⁰

Diese sehr enge⁶⁵¹ Definition hat das Gericht in aktuelleren Entscheidungen wiederholt.⁶⁵² Das spricht dafür, dass die Prüfung, inwieweit die Nachrichtendienste in den Bereich der nationalen Sicherheit fallen, zukünftig anhand dieser Definition erfolgen muss.⁶⁵³ Sie lässt sich in folgende Aspekte aufteilen:

aa) Schutzobjekt

Der erste Aspekt betrifft das Objekt, zu dessen Schutz ein Staat im Anwendungsbereich der nationalen Sicherheit tätig werden darf: die „wesentlichen Funktionen“ des Staates und die „grundlegenden Interessen“ der Gesellschaft sollen geschützt werden. Nicht jegliche Funktionen des Staates und nicht alle Interessen der Gesellschaft sind erfasst,

⁶⁴⁹ EuGH C-306/21 v. 20.10.2022 Koalitsia „Demokraticna Bulgaria – Obedinenie“, Rn. 40; EuGH C-439/19 v. 22.6.2021 Latvijas Republikas Saeima [Strafpunkte], Rn. 67.

⁶⁵⁰ EuGH C-511/18, C-512/18, C-520/18 v. 6.10.2020 *La Quadrature du Net*, Rn. 135; EuGH C-623/17 v. 6.10.2020 *Privacy International*, Rn. 74.

⁶⁵¹ *Bäcker*, Beschwerdeschrift BNDG II, S. 64; *Peuker*, EuR 2023, 535, 549.

⁶⁵² EuGH, C-140/20 v. 5.4.2022 G.D., Rn. 61; EuGH C-793/19, C-794/19 v. 20.9.2022 *SpaceNet und andere*, Rn. 92.

⁶⁵³ Nicht näher begründete Feststellungen, wonach die Nachrichtendienste per se unter die nationale Sicherheit subsumierbar sind, sind mit dieser neueren Rechtsentwicklung unmöglich geworden.

sondern nur die Wesentlichen und Grundlegenden. Mit Maßnahmen der nationalen Sicherheit können daher nur eng begrenzte Objekte geschützt werden.

bb) Art der staatlichen Reaktion

Zweitens beschreibt der EuGH die staatliche Reaktion, mit der das Schutzobjekt geschützt wird, als nicht näher ausdifferenzierte „Verhütung und Repression“ bestimmter Tätigkeiten, also relativ offen.

cc) Drohende Schäden⁶⁵⁴

Drittens nennt das Gericht drohende Schäden, welche die staatliche Reaktion in dieser Konstellation rechtfertigen.

(1) Art der Schäden

Es geht um solche Handlungen, die „geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen“. Auch im Zusammenhang mit den drohenden Schäden benutzt das Gericht eingrenzende Kriterien, da nicht jegliche Strukturen bestimmter Bereiche erfasst sind, sondern nur die „Tragenden“. Überzeugende Gründe sprechen darüber hinaus dafür, dass das „und“ kumulativ gemeint ist und daher die Gesellschaft, die Bevölkerung und der Staat als solcher neben der Destabilisierung unmittelbar bedroht sein müssen: Erstens hätte das Gericht statt dem „und“ ein „oder“ wählen können, wenn es hätte Optionen aufzeigen wollen. Zweitens wäre das einschränkende Kriterium der Unmittelbarkeit bedeutungslos, wenn es sich um zwei Alternativen handelte, da die erste Alternative geringere Voraussetzungen hätte, sich inhaltlich aber auf dasselbe bezieht.

(2) „Unmittelbar“

Mit welcher Bedeutung der EuGH den Begriff „unmittelbar“ hier verwendet, ist offen. Etymologisch kann er erstens meinen, dass kein oder kaum zeitlicher oder räumlich trennender Abstand vorhanden ist.⁶⁵⁵ Teilweise wird der Begriff im Kontext dieser Definition als ein Mangel an zeitlichem Abstand verstanden, in dem eine Bedrohung

⁶⁵⁴ Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9b.

⁶⁵⁵ <https://www.duden.de/rechtschreibung/unmittelbar> (abgerufen am 31.8.2024).

schon konkret erkennbar ist. Bei durch den Verfassungsschutz beobachteten Bestrebungen, die weder gewalttätig oder sonst rechtswidrig handeln noch Aussicht auf Erfolg haben, wäre die Unmittelbarkeit dann zu verneinen.⁶⁵⁶

Darüber hinaus könnte der Begriff mit der Bedeutung als „direkt“ im Sinne von „nicht mittelbar“, ohne temporale Aussage, verwendet worden sein.⁶⁵⁷ Dann wäre eine Bedrohung mittelbar, wenn sie beispielsweise gegen eine private Einrichtung oder Unternehmen gerichtet ist. Hier ist der Staat betroffen, weil er für die Sicherheit Privater (mit-)verantwortlich ist. Bei IT-gestützter Wirtschaftsspionage gegen ein privates Unternehmen beispielsweise wäre der Staat unter anderem deshalb mittelbar betroffen, weil seine Strafverfolgungsorgane für die Aufklärung zuständig sind. Unmittelbar wäre eine Bedrohung nach dieser Interpretation, wenn Vertreter des Staates oder staatlicher Einrichtungen selbst betroffen sind. In dem Beispiel würde sich das Hacking direkt gegen eine staatliche Behörde richten.

Wie genau der EuGH den Begriff verwenden wollte, kann leider auch durch Konsultation der französischen und englischen Fassung der Entscheidungen nicht geklärt werden. Statt dem Begriff „unmittelbar“ werden im Französischen und Englischen die Begriffe „directement“⁶⁵⁸ und „directly“⁶⁵⁹ verwendet. Beide können wie das deutsche „unmittelbar“ sowohl mit als auch ohne temporale Aussage genutzt werden.⁶⁶⁰

Gegen die erstgenannte Interpretation als zeitliche Eingrenzung spricht, dass für die Abwehr konkret absehbarer Bedrohungen die Polizeibehörden zuständig sind, für deren Tätigkeit jedoch – jedenfalls was die polizeiliche Zusammenarbeit und datenschutzrechtliche Aspekte angeht – der Anwendungsbereich des Unionsrechts bejaht und eine Regelungskompetenz des europäischen Gesetzgebers angenommen wird (vgl. insoweit z.B. die RL (EU) 2016/680)⁶⁶¹. Wenn die Polizei konkret erkennbare, schwerwiegende

⁶⁵⁶ Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9 d.

⁶⁵⁷ <https://www.duden.de/rechtschreibung/unmittelbar> (abgerufen am 31.8.2024).

⁶⁵⁸ EuGH C-511/18, C-512/18, C-520/18 vom 6.10.2020 La Quadrature du Net, Rn. 135, französische Fassung: <https://curia.europa.eu/juris/document/document.jsf?jsessionid=2EA79302AF2FE99BE73118CCD1EFA391?text=&docid=232084&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=375456> (abgerufen am 31.8.2024); EuGH C-623/17 v. 6.10.2020 Privacy International, Rn. 74, französische Fassung: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=390435>, (abgerufen am 31.8.2024).

⁶⁵⁹ EuGH C-623/17 v. 6.10.2020 Privacy International, Rn. 74, englische Fassung: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=392989> (abgerufen am 31.8.2024).

⁶⁶⁰ <https://www.cnrtl.fr/definition/directement> (abgerufen am 31.8.2024); <https://dictionary.cambridge.org/de/worterbuch/englisch/directly> (abgerufen am 31.8.2024).

⁶⁶¹ Pfeffer, Verfassungsblog vom 28.4.2021.

Bedrohungen für die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft, verhütet oder verfolgt, wäre das Unionsrecht nach dieser Interpretation nicht anwendbar. So kann es der EuGH jedoch nicht gemeint haben, denn dann würde er geltendem Unionsrecht widersprechen.

Dieser Einwand kann allerdings auch gegenüber der zweiten Interpretation erhoben werden: weil die Abwehr von schwerwiegenden Bedrohungen, die direkt gegen den Staat gerichtet sind, auch die Aufgabe des polizeilichen Staatsschutzes ist, würde diese Interpretation bedeuten, dass der Anwendungsbereich des Unionsrechts insoweit für die Polizeibehörden nicht eröffnet ist, was ebenfalls geltendem Unionsrecht widersprechen würde.

Im Ergebnis kann diese sprachliche Unschärfe zum jetzigen Zeitpunkt nicht aufgelöst werden und es bedarf einer Klarstellung des EuGH. Letztlich wäre die Definition besser handhabbar, wenn der Begriff „unmittelbar“ gestrichen würde.

Im Folgenden wird die Tätigkeit deutscher Nachrichtendienste unter beide Interpretationen subsumiert und kenntlich gemacht, welche Bedeutung angenommen wird.

(3) Beispiel der „terroristischen Aktivitäten“

Die „terroristischen Aktivitäten“ nennt der EuGH beispielhaft. Das bedeutet zunächst, dass andere Fallgruppen denkbar sind und die drohenden Schäden nur beschrieben, nicht abschließend definiert werden. Weiterhin folgt daraus, dass alle drohenden Schäden, die darunter subsumiert werden, mit terroristischen Aktivitäten zumindest vergleichbar sein müssen. Wann terroristische Straftaten im unionsrechtlichen Sinne vorliegen, richtet sich nach der RL (EU) 2017/541.⁶⁶² Deren Art. 3 enthält eine Liste von schweren Straftaten, bei denen es sich um terroristische Straftaten handelt, wenn sie mit einem der folgenden Ziele begangen werden: erstens die Bevölkerung auf schwerwiegende Weise einzuschüchtern, zweitens öffentliche Stellen oder eine internationale Organisation rechtswidrig zu einem Tun oder Unterlassen zu zwingen oder drittens die politischen, verfassungsrechtlichen oder sozialen Grundstrukturen eines Landes oder einer internationalen Organisation ernsthaft zu destabilisieren oder zu zerstören. Solche Straftaten sind beispielsweise Angriffe auf das Leben oder die körperliche Unversehrtheit einer Person, Entführungen, das Kapern von Verkehrsmitteln oder das Androhen solcher Straftaten. Gemäß Erwägungsgrund 14 der Richtlinie sind terroristische Aktivitäten alle Handlungen, die mit terroristischen Zwecken verbunden sind, zum Beispiel „die Anwerbung und Ausbildung oder Reisen“.

⁶⁶² In europäischen Dokumenten wird wiederholt auf diese Richtlinie verwiesen, z.B. in https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf (abgerufen am 31.8.2024), S. 6; so auch *Peuker*, EuR 2023, 535, 549.

c. Tätigkeiten der Nachrichtendienste im Anwendungsbereich des Unionsrechts

Ob die Datenverarbeitungen der Nachrichtendienste in den Anwendungsbereich des Unionsrechts fallen, richtet sich danach, ob ihre Aufträge und Tätigkeiten unter die maßgebliche Definition des EuGH subsumierbar sind.

aa) Spezifische Eigenschaften der staatlichen Reaktion zur Abgrenzung erforderlich?

Zunächst ist jedoch festzustellen, dass die Europäischen Union auch im Bereich der nationalen Sicherheit über Kompetenzen verfügt. So reguliert sie unter anderem die Terrorismusbekämpfung, beispielsweise mit der gerade erwähnten RL (EU) 2017/541. Daraus schließt *Bäcker*, dass die Definition zur Abgrenzung um einen Aspekt ergänzt werden muss. Es sei nicht ausreichend, in der Definition nur die drohenden Schäden zu benennen. Daneben seien „spezifische Eigenschaften der staatlichen Reaktion“ auf die drohenden Schäden notwendig. Ohne diesen zusätzlichen Aspekt könne nicht erklärt werden, wieso der polizeiliche Staatsschutz nach der oben genannten Definition die nationale Sicherheit schützt und dennoch in den Anwendungsbereich der Richtlinie 2016/680 und somit des Unionsrechts fällt.⁶⁶³

Was könnten solche spezifischen Eigenschaften staatlicher Reaktion sein? Das aus der Definition abgeleitete Schutzobjekt der staatlichen Maßnahme als solches kommt als Abgrenzungskriterium nicht in Frage, denn wie das obige Beispiel illustriert, kann auch die Polizei zum Schutz der wesentlichen Strukturen des Staates und der grundlegenden Interessen der Gesellschaft tätig werden. Auch ein rein formales Kriterium, das danach fragt, welche Behörde beauftragt ist (im Beispiel: Gefahrenabwehr- und Strafverfolgungsbehörde oder Nachrichtendienst), taugt nicht als eine solche Eigenschaft.⁶⁶⁴ Zum einen wäre den Mitgliedstaaten durch Kompetenzzumteilung dann jederzeit die „Flucht“ in den Bereich der nationalen Sicherheit möglich, um eine Materie unionsrechtlichen Vorgaben zu entziehen. Dies hätte zur Folge, dass ein unionsrechtlich zu definierender Begriff der nationalen Auslegung überlassen würde. Zum anderen grenzt das Unionsrecht selbst nicht rein formal nach der handelnden Behörde, sondern den verfolgten Aufgaben ab, vgl. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 RL (EU) 2016/680. Auch der EuGH bezieht sich nicht darauf.

In bestimmten Fällen kann stattdessen eine Negativabgrenzung hilfreich sein: Wo erstens explizit unionsrechtliche Kompetenzen bestehen und zweitens Sekundärrecht

⁶⁶³ Wolff/Brink/*Bäcker*, Art. 2 DSGVO Rn. 9b, der die Terrorismusbekämpfung und die RL (EU) 2017/541 als weiteres Beispiel nennt, in dem die Europäische Union Sekundärrecht im Bereich der nationalen Sicherheit erlässt.

⁶⁶⁴ So aber Wolff, der davon ausgeht, dass Art. 4 EUV institutionell abgrenzt und die Behördenzuständigkeit entscheidend ist, Wolff/Brink/*Wolff*, § 45 BDSG Rn. 21.

erlassen wurde, unter welches die staatliche Reaktion subsumiert werden kann, erfüllt die staatliche Reaktion die notwendige spezifische Eigenschaft jedenfalls nicht. Mit „spezifischen Eigenschaften der staatlichen Reaktion“ sind somit solche behördlichen Tätigkeitsfelder gemeint, die gerade nicht unmittelbar auf die Durchsetzung einer unional vorgeprägten Vorschrift gerichtet sind.

bb) Schutzobjekt

Die Tätigkeit der Nachrichtendienste ist an eng definierte Aufträge gebunden⁶⁶⁵, die über das vom EuGH definierte Objekt, die wesentlichen Strukturen des Staates und nicht mehr als die grundlegenden Interessen der Gesellschaft zu schützen, grundsätzlich⁶⁶⁶ nicht hinausgehen.

cc) Art der staatlichen Reaktion

Nach ihrem Aufklärungsauftrag sollen die Nachrichtendienste etwaige Bedrohungen möglichst früh entdecken, um sie an die Regierung oder die Strafverfolgungs- und Gefahrenabwehrbehörden weiterleiten zu können. Somit dient ihre Tätigkeit der Verhütung von Bedrohungen im Sinne der Definition.

dd) Drohende Schäden

Nicht alle Tätigkeiten der Nachrichtendienste sind auf die Verhütung der eng begrenzten, drohenden Schäden im Sinne der Definition des EuGH ausgerichtet.

(1) Weit gefasster Auftrag des BND

Der Aufklärungsauftrag des BND erstreckt sich auf sämtliche Gegenstände, die für die außen- und sicherheitspolitischen Entscheidungen der Bundesregierung relevant sein können. Die Bundesregierung soll auf diese Weise in die Lage versetzt werden, möglichst informierte Entscheidungen zu treffen, die im Zusammenhang mit etwaigen Bedrohungen stehen können, aber nicht zwangsläufig auf Bedrohungen bezogen sein müssen. So sind Überwachungen zur politischen Unterrichtung der Bundesregierung auch zur Aufklärung über wirtschaftliche und kulturelle Vorgänge von außen- und sicherheitspolitischer Bedeutung möglich.⁶⁶⁷

⁶⁶⁵ Vgl. [Teil 1 B. II.](#)

⁶⁶⁶ Hinsichtlich welcher Aspekte dies in Frage zu stellen ist, wird unter „dd) Drohende Schäden“ diskutiert.

⁶⁶⁷ Bäcker, Beschwerdeschrift BNDG II, S. 64.

Die Datenverarbeitung des BND dient damit nicht generell der Verhütung von Schäden gemäß der Definition, sodass dessen Tätigkeit teilweise in den Anwendungsbereich des Unionsrechts fällt.

(2) Allgemeine Bekämpfung der organisierten Kriminalität

Ob die Bekämpfung jeglicher Formen organisierter Kriminalität der Verhütung von solchen Schäden dient, ist zweifelhaft.⁶⁶⁸ Insbesondere kann nicht davon ausgegangen werden, dass organisierte Kriminalität durchweg in der Lage wäre, die tragenden Strukturen in den Bereichen Verfassung, Wirtschaft, Politik oder im sozialen Bereich schwerwiegend zu destabilisieren. Es liegt nahe, dass organisierte Kriminalität nur im Einzelfall ein Ausmaß annimmt, bei dem beispielsweise eine „ungesetzliche Beeinträchtigung“⁶⁶⁹ der Amtsführung von Verfassungsorganen zu befürchten ist. Nur in solchen und vergleichbaren Situationen ist jedoch eine schwerwiegende Destabilisierung tragender Strukturen möglich. Zudem ist fraglich, ob die Gesellschaft, die Bevölkerung oder der Staat selbst durch jegliche organisierte Kriminalität unmittelbar bedroht sind. Mit terroristischen Aktivitäten vergleichbar sind Handlungsformen organisierter Kriminalität grundsätzlich nicht, da sie vorwiegend auf Gewinnerzielung und nicht auf eine der in Art. 3 Abs. 2 RL (EU) 2017/541 definierten Ziele ausgerichtet sind.

Ob ausschließlich schwerwiegende Formen organisierter Kriminalität beobachtet werden, die unter die Definition der nationalen Sicherheit subsumiert werden können, kann abschließend nur beantworten, wer in den Nachrichtendiensten, Ministerien und Parlamenten über Zugang zu den als geheim eingestuften Informationen verfügt. Dennoch ermöglichen die öffentlich zugänglichen Aussagen in den Verfassungsschutzberichten indizielle Rückschlüsse. Auf ihrer Basis entsteht der Eindruck, dass die in Folge der darin beschriebenen Formen organisierter Kriminalität drohenden Schäden mit den Anforderungen des EuGH nicht vergleichbar sind:

So ergibt sich aus dem bayerischen Verfassungsschutzbericht von 2023 beispielsweise, dass beobachtete Rockergruppierungen untereinander Gebietsansprüche erhoben haben und „interne Streitigkeiten“ mitunter mit Waffen austrugen, weiter heißt es, regional sei es zu Gewalttaten gekommen, während die „Lage in Bayern (...) eher ruhig“ war.⁶⁷⁰

Laut dem hessischen Verfassungsschutzbericht 2022 sind die Schwerpunkte der Rockerkriminalität Gebietsansprüche, vor allem in Bezug auf Menschenhandel und

⁶⁶⁸ Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9b; Bäcker, Beschwerdeschrift BNDG II, S. 64.

⁶⁶⁹ Gusy, StV 1995, 320, 325.

⁶⁷⁰ Verfassungsschutzbericht Bayern 2023, https://www.verfassungsschutz.bayern.de/mam/anlagen/vsb-2023_nicht_barrierefrei.pdf, S. 341 (abgerufen am 31.8.2024).

Zwangsprostitution. In Bezug auf die italienische organisierte Kriminalität seien die Geldwäsche, der internationale Kokainhandel und Schutzgelderpressung bei italienischen Restaurantbetreibern „deliktische Schwerpunkte“.⁶⁷¹

Wo punktuell (mitunter schwere) Verbrechen begangen werden, liegt die Destabilisierung tragender Strukturen des Staates noch in weiter Ferne.

Im Ergebnis (und unter Vorbehalt von Verschlussachen, die womöglich etwas Gegenteiliges beweisen) ist daher davon auszugehen, dass die generelle Beobachtung organisierter Kriminalität durch die Landesämter für Verfassungsschutz in Bayern, Hessen und dem Saarland⁶⁷² mangels vergleichbar schwerer, drohender Schäden unter die nationale Sicherheit nicht subsumierbar sind und diese Tätigkeit somit in den Anwendungsbereich des Unionsrechts fallen.

(3) „Unmittelbare“ Bedrohung bei jeglicher Vorfeldaufklärung?

Falls der Begriff der „unmittelbaren“ Bedrohung als konkret absehbare Bedrohung verstanden wird, stellt sich die Frage, inwieweit die Nachrichtendienste im Rahmen ihrer Vorfeldaufklärung solche Bedrohungen verhüten.

Bäcker weist darauf hin, dass der Verfassungsschutz gem. § 3 Abs. 1 Nr. 1 BVerfSchG Bestrebungen, die sich gegen die freiheitlich-demokratische Grundordnung richten, beobachtet, und dass solche Bestrebung bereits bei aktivem, ziel- und zweckgerichtetem Vorgehen⁶⁷³ zu bejahren sind, „gewalttätige oder sonst rechtswidrig Handlungen“ oder „eine Erfolgsaussicht der Bestrebung“ seien gerade nicht erforderlich. Dementsprechend erfasse der Auftrag des Verfassungsschutzes auch solche „verfassungsfeindliche Strukturen, bei denen es an der vom EuGH vorausgesetzten unmittelbaren Bedrohungslage fehlt“.⁶⁷⁴

Dem ist zuzustimmen. Die Schlussfolgerung trifft für vergleichbare Tätigkeiten des MAD ebenso zu. Manche Beobachtungsobjekte des Verfassungsschutzes und des MAD, insbesondere solche, denen jede Aussicht auf Erfolg fehlt, sind damit unter den Begriff der nationalen Sicherheit nicht subsumierbar. Dies hat zur Folge, dass auf diese Tätigkeiten das einschlägige Unionsrecht anwendbar ist.

Der BND wird grundsätzlich noch weiter im Gefahrenvorfeld tätig, ob beobachtete Handlungen illegal sind, ist unerheblich.⁶⁷⁵ Die Aufklärungstätigkeit des BND ist daher

⁶⁷¹ Verfassungsschutz in Hessen, Bericht 2022, https://verfassungsschutz.hessen.de/sites/verfassungsschutz.hessen.de/files/2023-11/lfv_bericht22_screen_neu_1123.pdf, S. 67, 295 (abgerufen am 31.8.2024).

⁶⁷² Vgl. [Teil 1 B. II. 3. b. aa.](#)

⁶⁷³ Vgl. [Teil 1 B. II. 3. a. aa. \(3\).](#)

⁶⁷⁴ Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9 d.

⁶⁷⁵ Vgl. [Teil 1 B. II. 1. b. aa.](#)

ebenfalls nicht bzw. jedenfalls nicht ausschließlich auf den Schutz vor unmittelbar drohenden Gefahren ausgerichtet und ist deshalb nicht von der Bereichsausnahme erfasst.

(4) Öffentlichkeitsarbeit und Prävention als Reaktion bei „unmittelbarer“ Bedrohung?

Auf den ersten Blick handelt es sich bei der Öffentlichkeitsarbeit des Verfassungsschutzes und den Präventionstätigkeiten mancher Landesverfassungsschutzämter unproblematisch um „Verhütung“ im Sinne der Definition des EuGH. Bezieht man in die Überlegung ein, dass unmittelbare Bedrohungen verhütet werden sollen, ist die Antwort weniger eindeutig.

Wenn „unmittelbar“ bedeutet, dass die von der Definition erfassten schwerwiegenden Bedrohungen bereits konkret erkennbar sind, erscheinen Öffentlichkeits- und Präventionsarbeit jedoch nicht als probates Mittel zur Verhütung der Bedrohung. Dann ist eine Informationsübermittlung an die Gefahrenabwehrbehörden oder eine Information der politischen Entscheidungsträger vielversprechender. Das Ansprechen einzelner Zielpersonen könnte zwar bei der Verhütung von Gefahren nutzen. Hier stellt sich aber die Frage, mit welchen Mitteln eine Behörde dies bewerkstelligen soll, die im Gegensatz zur Polizei über keinerlei operative Befugnisse verfügt. Dies spricht dafür, dass diese Tätigkeiten stattdessen der Verhütung von Bedrohungen dienen, die sich langfristig zu realisieren drohen. Die Öffentlichkeitsarbeit in Form des jährlich erscheinenden Tätigkeitsberichts ist schon wegen ihres Erscheinungsrhythmus ein untaugliches Mittel, bereits konkret erkennbaren Bedrohungen zu begegnen.

Damit fallen sowohl die Öffentlichkeitsarbeit als auch die sonstige Prävention in den Anwendungsbereich des Unionsrechts.

ee) Zwischenergebnis

Mit der neuen Definition des EuGH ist es unmöglich geworden, die Tätigkeit der Nachrichtendienste – mit der formalen Begründung, dass es sich um Nachrichtendienste handelt – vollständig unter den Begriff der nationalen Sicherheit zu subsumieren und somit dem Anwendungsbereich des Unionsrechts zu entziehen. Stattdessen ist entscheidend, inwieweit die Tätigkeit der Nachrichtendienste unter die Definition gefasst werden kann. Die Definition ist in drei Aspekte zu unterteilen: erstens das Schutzobjekt, zweitens die Art der staatlichen Reaktion und drittens die drohenden Schäden. Darüber hinaus sind konfligierende Kompetenzen der Union zur Abgrenzung heranzuziehen.

Die Tätigkeit der Nachrichtendienste unter die „drohenden Schäden“ zu subsumieren, ist kompliziert. Da der Auftrag des BND nicht auf die Verhütung von Bedrohun-

gen begrenzt ist, ist dessen Tätigkeit von der nationalen Sicherheit im Sinne der Definition jedenfalls nicht vollständig gedeckt. Fest steht außerdem, dass die Verhütung jeglicher Formen organisierter Kriminalität nicht mit den vom EuGH definierten drohenden Schäden vergleichbar und somit kein Bestandteil der nationalen Sicherheit ist.⁶⁷⁶

Demgegenüber wirft der Begriff der „unmittelbar“ bedrohenden Tätigkeiten Interpretationsprobleme auf: Er könnte einerseits als im zeitlichen Sinne bereits konkret erkennbare, bedrohende Tätigkeiten oder als „nicht mittelbar“ bedrohende Tätigkeiten verstanden werden.⁶⁷⁷ In der ersten Interpretationsweise sind weite Teile der nachrichtendienstlichen Vorfeldaufklärung nicht darunter subsumierbar, da diese Bedrohungen stattdessen im Aufgabenbereich der operativ tätigen Gefahrenabwehrbehörden verortet sind.⁶⁷⁸ Auch die Öffentlichkeitsarbeit und sonstige Prävention durch den Verfassungsschutz dient nicht der Verhütung von bereits konkret erkennbaren Bedrohungen, weshalb diese Tätigkeiten in den Anwendungsbereich des Unionsrechts fielen.

Im Ergebnis kann die Arbeit der Nachrichtendienste nicht länger generell unter Art. 4 Abs. 2 S. 3 EUV gefasst werden. Das bedeutet jedoch nicht, dass jede nachrichtendienstliche Tätigkeit in den Anwendungsbereich des Unionsrechts fällt. Stattdessen zwingt die Definition zu einer differenzierten Betrachtung.

d. Negative Auswirkung der Definition

Es ist offensichtlich, dass die Subsumtion unter die Definition des EuGH zur nationalen Sicherheit aus den Entscheidungen *La Quadrature du Net und andere* sowie *Privacy International* vom 6. Oktober 2020 kompliziert ist. Auf das deutsche Nachrichtendienstrecht angewandt, führt die enge Definition des EuGH dazu, dass Teile der nachrichtendienstlichen Aufgaben in den Anwendungsbereich des Unionsrechts fallen und andere nicht. Während es bei der Präventionstätigkeit gem. einiger Landesverfassungsschutzgesetze⁶⁷⁹ vergleichsweise einfach sein dürfte, das Unionsrecht anzuwenden, stellt sich die Frage, wie der Gesetzgeber damit umgehen soll, wenn beispielsweise für weite Teile der Vorfeldaufklärung Unionsrecht gilt, während für andere Tätigkeitsbereiche rein nationale Maßstäbe gelten. Mithin führt die Anwendung der Definition des EuGH dazu, dass eine schwer durchschaubare Rechtsmaterie noch komplexer wird.

⁶⁷⁶ So auch Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9 b.

⁶⁷⁷ Vgl. [Teil 2 B. II. 1. b. cc](#)) (2).

⁶⁷⁸ Umgekehrt geht damit einher, dass Tätigkeiten der Gefahrenabwehrbehörde, die unter die Definition subsumierbar sind, in den Anwendungsbereich der nationalen Sicherheit und somit aus dem Anwendungsbereich des Unionsrechts fallen können. Der Gesetzgeber differenziert de lege lata nicht.

⁶⁷⁹ Vgl. [Teil 1 B. II. 3. b. cc](#)); § 5 Abs. 2 [VerfSchG MV](#), § 5 Abs. 1 [ThürVerfSchG](#), § 4a [VerfSchG-LSA](#), § 3 Abs. 3 [NVerfSchG](#); § 3 Abs. 3 [VSG NRW](#).

Ob der EuGH die Folgewirkungen seiner Definition abschätzen konnte, ist unklar. Er hatte jedoch keine andere Wahl als den Begriff der nationalen Sicherheit begrifflich zu schärfen, weil er den Ausnahmetatbestand gem. Art. 15 Abs. 1 i. V. m. Art. 1 Abs. 3 RL (EU) 2002/58 handhabbar machen musste.

Soweit der EuGH zukünftig an dieser engen Definition festhält, gelten unionsrechtliche Maßstäbe auch in Teilen des Nachrichtendienstrechts. Für die Handhabbarkeit und Nachvollziehbarkeit des Rechtsgebiets wäre es dann am sinnvollsten, dass der deutsche Gesetzgeber – überobligatorisch – die gesamte Tätigkeit der Nachrichtendienste an europäischem Sekundärrecht ausrichtet; und es nicht nur für die Bereiche anwendet, in denen die Definition ihn dazu zwingt.

e. Aktuellere Definition des EuGH?

In einer Entscheidung vom 16. Januar 2024 hat der EuGH bei der Auslegung der nationalen Sicherheit allerdings nicht auf diese detaillierte Definition zurückgegriffen. Stattdessen hat er eine kürzere Formel angewandt, die bereits aus früheren Entscheidungen bekannt ist: auf die „Wahrung der nationalen Sicherheit abzielend[e] Tätigkeiten“ seien demnach „insbesondere solche, die den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft bezwecken“.⁶⁸⁰

In der Entscheidung ging es unter anderem darum, ob ein Untersuchungsausschuss, der prüft, ob das österreichische Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) in unzulässiger Weise politisch beeinflusst worden ist, an die DSGVO gebunden ist oder ob die Bereichsausnahme gem. Art. 2 Abs. 2 lit. a) DSGVO anwendbar ist, weil diese Tätigkeit unter die nationale Sicherheit subsumierbar ist und damit nicht in den Anwendungsbereich des Unionsrechts fällt. Der EuGH stellt fest, dass eine Tätigkeit entweder der nationalen Sicherheit dienen muss oder „derselben Kategorie“ zuordenbar sein muss, was er in Bezug auf die politische Kontrolle durch den Untersuchungsausschuss verneinte. Soweit der Untersuchungsausschuss Zugang zu Informationen habe, die wegen der nationalen Sicherheit schützenswert seien, habe der Gesetzgeber gem. Art. 23 DSGVO die Möglichkeit, Ausnahmen von den Rechten und Pflichten der DSGVO zu normieren.⁶⁸¹

Ohne darauf näher einzugehen, hat der EuGH in Bezug auf das BVT festgestellt, dass dessen Tätigkeit größtenteils unter die nationale Sicherheit fällt:

⁶⁸⁰ EuGH C-33/22 v. 16.1.2024 Österreichische Datenschutzbehörde, Rn. 46 m. Verweis auf EuGH C-306/21 v. 20.10.2022 Koalitsia „Demokraticna Bulgaria – Obedinenie“, Rn. 40; EuGH C- 439/19 v. 22.6.2021 Latvijas Republikas Saeima [Strafpunkte], Rn. 67.

⁶⁸¹ EuGH C-33/22 v. 16.1.2024 Österreichische Datenschutzbehörde, Rn. 48, 52 f.; hierzu auch Ehmann/Selmayr/Zerdlack Art. 2 DSGVO Rn. 8.

„*Insoweit reicht* der Umstand, dass der Verantwortliche eine Behörde ist, deren Haupttätigkeit in der Gewährleistung der nationalen Sicherheit besteht, als solcher nicht aus, um Verarbeitungen personenbezogener Daten durch diese Behörde im Rahmen anderer von ihr durchgeführter Tätigkeiten vom Anwendungsbereich der DSGVO auszunehmen.“⁶⁸²

Demnach fällt zumindest „die Haupttätigkeit“ des BVT unter die Ausnahme der nationalen Sicherheit. Das vorliegende Gericht bezeichnet das BVT zwar als „polizeiliche Staatsschutzbehörde“, das BVT war jedoch auch der österreichische Inlandsnachrichtendienst⁶⁸³. Die Entscheidung spricht daher dafür, dass zumindest „die Haupttätigkeit“ der Nachrichtendienste unter die nationale Sicherheit subsumierbar ist und damit nicht in den Anwendungsbereich des Unionsrechts fällt.

Allerdings begründet der EuGH diese Aussage nicht. Offen ist auch, ob er die Tätigkeit (gedanklich) unter die in dieser Entscheidung zitierte, verkürzte Definition subsumiert hat und deshalb zu diesem Ergebnis kommt, und ob zukünftig anstatt der ausführlicheren Definition aus der Entscheidung zu *Privacy International* 6.10.2020⁶⁸⁴ diese Definition maßgeblich ist. Da die Haupttätigkeit der deutschen Nachrichtendienste den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft bezweckt, wäre sie nach Maßgabe dieser Definition vom Unionsrecht nicht erfasst.

Es bleibt abzuwarten, welche der zwei Definitionen der EuGH zukünftig verwenden wird.

2. *Einschlägiges Sekundärrecht: DSGVO oder JIRL?*

Bezogen auf die nachrichtendienstlichen Tätigkeiten, die nach der ausführlichen Definition des EuGH in der Entscheidung zu *Privacy International*⁶⁸⁵ in den Anwendungs-

⁶⁸² EuGH C-33/22 v. 16.1.2024 Österreichische Datenschutzbehörde, Rn. 51.

⁶⁸³ <https://www.derstandard.at/story/2000131534015/das-bvt-ist-geschichte-der-neue-verfassungsschutz-dsn-startet>, (abgerufen am 31.8.2024).

⁶⁸⁴ Vgl. [Teil 2 B. II. 1. b.](#); EuGH C-623/17 v. 6.10.2020 *Privacy International*, Rn. 74; EuGH C-511/18, C-512/18, C-520/18 v. 6.10.2020 *La Quadrature du Net*, Rn. 135.

⁶⁸⁵ Vgl. [Teil 2 B. II. 1. b.](#); EuGH C-623/17 v. 6.10.2020 *Privacy International*, Rn. 74; EuGH C-511/18, C-512/18, C-520/18 v. 6.10.2020 *La Quadrature du Net*, Rn. 135.

bereich des Unionsrechts fallen, also die allgemeine Beobachtung der organisierten Kriminalität, Teile der Tätigkeit des BND und – gegebenenfalls⁶⁸⁶ – die Vorfeldaufklärung ohne Bezug zu einer sofortigen Bedrohung, könnten die DSGVO oder die JIRL einschlägig sein.

a. Anwendbarkeit der JIRL

Zunächst ist zu klären, ob die Nachrichtendienste in den Anwendungsbereich der spezielleren JIRL fallen.⁶⁸⁷ Gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 gilt die JIRL für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden „zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“. Die von den Nachrichtendiensten gesammelten Daten beziehen sich auf identifizierte oder identifizierbare Personen und sind daher personenbezogen (Art. 3 Nr. 1 JIRL).⁶⁸⁸ Darüber hinaus müssten die Daten entweder ganz oder teilweise automatisiert verarbeitet oder nichtautomatisiert verarbeitet und in einem Dateisystem gespeichert werden (Art. 2 Abs. 2, Art. 3 Nr. 2, 6 JIRL). Wenn Akten nach gewissen Kriterien angelegt werden, ist die „Speicherung in einem Dateisystem“ bereits zu bejahen.⁶⁸⁹ In Folge der Digitalisierung und der damit verbundenen Speicherung in Datenbanken wird in der Regel eine (teil-)automatisierte Verarbeitung vorliegen.⁶⁹⁰ Schwieriger zu beantworten ist hingegen, ob die Nachrichtendienste als Kriminalbehörden im Sinne der Norm einzuordnen sind.⁶⁹¹

aa) Auslegung von Art. 1 Abs. 1 JIRL

Zuständige Behörde ist gem. Art. 3 Nr. 7 JIRL, wer als staatliche Stelle Aufgaben gem. Art. 1 Abs. 1 JIRL verfolgt (aufgabenbezogener Behördenbegriff⁶⁹²). Die Begriffe in

⁶⁸⁶ Insoweit kommt es darauf an, wie der EuGH den Begriff der „unmittelbaren“ Bedrohung interpretiert, vgl. [Teil 2 B. II. 1. c. dd\) \(4\)](#).

⁶⁸⁷ Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9 d.

⁶⁸⁸ Außerdem ist denkbar, dass die Informationen sich auf juristische Personen beziehen. Selbst dann ist jedoch davon auszugehen, dass Daten über dahinterstehende natürliche Personen mitverarbeitet werden. Personenbezogene Einschätzungen einer Sicherheitsbehörde über einzelne Personen (z.B. als „Gefährder“) sind personenbezogene Daten, Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 969 Rn. 431.

⁶⁸⁹ Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 972, Rn. 443; Wolff/Brink/Albers, Datenschutzbestimmungen der Polizei- und Nachrichtendienstgesetze des Bundes Rn. 48.

⁶⁹⁰ Zur insoweit vergleichbaren Polizeiarbeit Wolff/Brink/Albers, Datenschutzbestimmungen der Polizei- und Nachrichtendienstgesetze des Bundes Rn. 48.

⁶⁹¹ Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9d.

⁶⁹² Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 972 Rn. 446.

Art. 1 Abs. 1 JIRL sind autonom unionsrechtlich auszulegen.⁶⁹³ Der unionsrechtliche Straftatenbegriff erstreckt sich auf Ordnungswidrigkeiten nach deutschem Recht.⁶⁹⁴ Die „öffentliche Sicherheit“ ist weitergehend als die „nationale Sicherheit“ und erfasst „den Erhalt der inneren und äußeren Sicherheit eines Mitgliedstaates, was den Schutz von Einrichtungen des Staates, wichtiger öffentlicher Dienste, kritischer Infrastrukturen, aber auch das Überleben der Bevölkerung, das friedliche Zusammenleben und militärische Interessen des Staates beinhaltet. Daneben sind auch die subjektiven Interessen und Rechtsgüter der Bevölkerung, etwa vor bandenmäßiger Kriminalität, geschützt.“⁶⁹⁵ Der Satzteil „einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“ ist eng auszulegen.⁶⁹⁶ Seine Voraussetzungen liegen nach *Bäcker* nur vor, wenn ein Bezug zur Straftatenverhütung oder -verfolgung gegeben ist: Dies ist dann der Fall, wenn der Schutz der öffentlichen Sicherheit neben der Straftatenverhütung bzw. -verfolgung eine zusätzliche Aufgabe darstellt und diese „in einem engen Zusammenhang mit der Bekämpfung von Straftaten“ steht, „so dass bei der Erfüllung der Aufgabe ein Übergang zur Verhütung oder Verfolgung von Straftaten typischerweise naheliegt.“⁶⁹⁷ Andere lassen einen „zumindest potentiellen Straftatbezug“ ausreichen.⁶⁹⁸

bb) Subsumtion der nachrichtendienstlichen Aufträge

Für die Subsumtion unter Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 JIRL ist entscheidend, welchen Zwecken die Datenverarbeitungen der Nachrichtendienste dienen. Ihre Aufgabe besteht zunächst darin, die Regierung zu informieren (politische Information). Der Verfassungsschutz soll zudem die Öffentlichkeit über verfassungsfeindliche Bestrebungen aufklären. Der BND ist darüber hinaus mit der Früherkennung aus dem Ausland drohender Gefahren beauftragt.⁶⁹⁹ Außerdem sind die Nachrichtendienste – un-

⁶⁹³ *Müller/Schwabenbauer*, Hdb. des Polizeirechts, 952, 974 Rn. 453; *Weinhold/Johannes*, DVBl 2016, 1501, 1503.

⁶⁹⁴ *Wolff/Brink/Bäcker*, Art. 2 DSGVO Rn. 25 a.

⁶⁹⁵ *Weinhold/Johannes*, DVBl 2016, 1501, 1503.

⁶⁹⁶ *Wolff/Brink/Bäcker*, Art. 2 DSGVO Rn. 29; *Golla*, KriPoZ 2019, 238; *Müller/Schwabenbauer*, Hdb. des Polizeirechts, 952, 975 Rn. 456.

⁶⁹⁷ *Bäcker*, Datenschutzrichtlinie für Polizei und Strafjustiz, 63, 66 f., vgl. zu anderen Ansichten überblicksartig: *Stevens/Limberger*, JZ 2022, 656, 657 m. w. N.: Teilweise wird eine institutionelle Abgrenzung vertreten, wonach Tätigkeiten von Polizei und Strafverfolgungsbehörden immer der JIRL unterfallen, teilweise soll nur die Abwehr solcher Gefahren darunter subsumierbar sein, bei deren Realisierung eine Straftat vorläge.

⁶⁹⁸ *Müller/Schwabenbauer*, Hdb. des Polizeirechts, 952, 975 Rn. 457.

⁶⁹⁹ Vgl. [Teil 1 B. II. 1. b. aa\)](#).

abhängig von ihrem Auftrag – als „Informationsdienstleister der operativen Sicherheitsbehörden“ jedenfalls funktional an der Abwehr konkreter Gefahren und der Aufklärung von Straftaten beteiligt.⁷⁰⁰

Vor diesem Hintergrund ergeben sich grundsätzlich vier Subsumtionsoptionen. Erstens könnten die Zwecke der „Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung“ gem. Art. 1 Abs. 1 JIRL weit ausgelegt werden. Im Rahmen dieser weiten Auslegung wäre es ausreichend, dass die Nachrichtendienste funktional an der Strafverfolgung beteiligt sind, wenn sich entsprechende Hinweise zu Straftaten als „Nebenprodukt“ der Informationssammlung ergeben und an die Strafverfolgungsbehörden übermittelt werden.

Zweitens könnte der Zweck der Straftatenverhütung und -verfolgung eng auszulegen sein. Dann wären die Aufträge der Nachrichtendienste gegebenenfalls unter den zusätzlichen Zweck des „Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“ subsumierbar. Die Nachrichtendienste schützen mittelbar und frühzeitig vor Gefahren für die öffentliche Sicherheit, indem sie die Regierung informieren. Jedenfalls in ihrer Funktion als Informationsdienstleister der operativen Sicherheitsbehörden könnten die Nachrichtendienste unter diese Variante subsumierbar sein. Der Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit ist jedoch eng auszulegen, es muss zumindest ein Bezug zur Straftatenverhütung vorliegen. Ob die funktionale Beteiligung an der Straftatenverfolgung die von *Bäcker* hierzu formulierten Anforderungen⁷⁰¹ erfüllt, ist offen. Ein Bezug zur Straftatenverhütung und -verfolgung existiert wie in der ersten Auslegungsvariante beschrieben dennoch: im Auftrag zur Übermittlung relevanter Informationen an die operativen Sicherheitsbehörden. Dafür, dass dies hier ausreichend sein könnte, spricht, dass es das Ziel der engen Auslegung ist, allgemeine Verwaltungstätigkeiten aus dem Anwendungsbereich der JIRL herauszuhalten und dem Anwendungsbereich der DSGVO zuzuordnen, um so das Harmonisierungsziel der DSGVO nicht zu gefährden.⁷⁰² Die Tätigkeit der Nachrichtendienste

⁷⁰⁰ *Bäcker*, Hdb. des Polizeirechts, 109, 152 Rn. 251; *Warg*, Hdb. des Rechts der Nachrichtendienste, 509, 518 Rn. 8.

⁷⁰¹ Vgl. [Teil 2 B. II. 1. c. aa](#)).

⁷⁰² „Zum Schutz vor Gefahren für die so verstandene öffentliche Sicherheit sind neben den Kriminalbehörden zahlreiche weitere Behörden berufen. Bei einem weiten Verständnis des Zusatzes in Art. 1 Abs. 1 DSRL-PSJ wären daher große Teile der Ordnungsverwaltung vom sachlichen Anwendungsbereich der Richtlinie umfasst – und dementsprechend vom sachlichen Anwendungsbereich der Datenschutz-Grundverordnung gemäß Art. 2 Abs. 2 lit. d DSGVO ausgenommen. Dies wäre mit dem Anliegen des reformierten europäischen Datenschutzrechts unvereinbar, den Datenschutz auch im öffentlichen Sektor zumindest überwiegend zu harmonisieren“, *Bäcker*, Datenschutzrichtlinie für Polizei und Strafjustiz, 63, 66.

ist mit den von den Befürwortern der engen Auslegung für die allgemeine Verwaltungstätigkeit genannten Beispielen wie der „Gewerbeaufsichts- oder Ausländerbehörde“⁷⁰³ oder „Waffen- oder Hygienebehörden“⁷⁰⁴ wegen ihrer Ausrichtung auf die Sicherheit von Grundlagen des Staates jedoch gerade nicht vergleichbar. Da der Zweck der sehr engen Auslegung von *Bäcker* (Gefährdung der Harmonisierungswirkung der DSGVO durch Einbeziehung der gesamten Ordnungsverwaltung) durch die spezielle nachrichtendienstliche Tätigkeit nicht verletzt werden kann, sollten die einschränkenden Voraussetzungen in diesem Zusammenhang nicht angewandt werden. Dies hätte zur Folge, dass das Sammeln von Informationen für die Regierung als Gefahrenabwehr mit Strafverfolgungsbezügen im Sinne des Zusatzes gem. Art. 1 Abs. 1 JIRL einzuordnen wäre.

Drittens könnte die Straftatenverhütung und -verfolgung eng zu verstehen und der Begriff der Gefahrenabwehr so restriktiv auszulegen sein, dass die mittelbare, im Vorfeld angesiedelte Gefahrenabwehr und Strafverfolgung durch Information der Regierung bzw. der operativ tätigen Behörden davon nicht gedeckt ist. Dann wäre der Anwendungsbereich der DSGVO eröffnet.

Viertens könnte man vertreten, dass die politische Information keine Gefahrenabwehr i. S. v. Art. 1 S. 1 JIRL ist. Dann müsste nach dem mit der jeweiligen Datenverarbeitung verbundenen Zweck differenziert werden. Werden Daten zur politischen Information verarbeitet, wäre demnach die DSGVO einschlägig.

Gegen die dritte Variante spricht, dass der Wortlaut von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 JIRL keinerlei Anhaltspunkte dafür enthält, dass der Zweck der Strafverfolgung oder Gefahrenabwehr nur bejaht werden kann, wenn die Behörde über operative Befugnisse verfügt. Das Mittel der Zweckverfolgung spielt gerade keine Rolle, entscheidend ist das Ziel. Gegen die vierte Option spricht, dass auch die politische Information im Ergebnis dem frühzeitigen Schutz vor Gefahren dient, zudem sind die Nachrichtendienste „funktional“ an der Gefahrenabwehr beteiligt⁷⁰⁵, sie betreiben „Gefahrenabwehr mittels Informationsverarbeitung“⁷⁰⁶.

Letztendlich sind die erste und zweite Auslegungsoption unter Berücksichtigung des Zwecks der JIRL am überzeugendsten. Die JIRL ist eine Spezialregelung für die Besonderheiten des Strafverfolgungs- und Gefahrenabwehrrechts, die insgesamt „soveränitätsschonender“⁷⁰⁷ ausgestaltet ist als die DSGVO:

⁷⁰³ *Bäcker*, Datenschutzrichtlinie für Polizei und Strafjustiz, 63, 67.

⁷⁰⁴ *Müller/Schwabenbauer*, Hdb. des Polizeirechts, 952, 975 Rn. 459.

⁷⁰⁵ *Warg*, Hdb. des Rechts der Nachrichtendienste, 509, 518.

⁷⁰⁶ „Gefahrenabwehr im weiteren Sinn“, *Schenke*, Polizei- und Ordnungsrecht, Rn. 445d, 438.

⁷⁰⁷ *Müller/Schwabenbauer*, Hdb. des Polizeirechts, 952, 976 Rn. 460; Möstl/Schwabenbauer/Schröder, Datenschutz-Richtlinie (EU) 2016/680 (JI-RL) Rn. 32.

Im Gegensatz zur Vollharmonisierung der DSGVO wird gem. Art. 1 Abs. 3 JIRL eine Mindestharmonisierung angestrebt, der Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a DSGVO fehlt, um heimliche Maßnahmen von Sicherheitsbehörden zu ermöglichen; außerdem sind die Befugnisse der Aufsichtsbehörden weniger weitreichend.⁷⁰⁸

Eine Materie wie das Nachrichtendienstrecht, die wegen ihrer Bedeutung für die nationale Sicherheit nach der herrschenden Meinung bis heute – trotz der klarstellenden Definition des EuGH – vollständig unter Art. 4 Abs. 2 S. 3 EUV subsumiert wird und damit in die alleinige Verantwortung der Mitgliedstaaten fällt, ist nicht weniger sensibel als das Strafverfolgungs- und Gefahrenabwehrrecht. Bei Anwendbarkeit der JIRL wäre der Transparenzgrundsatz wegen der heimlichen Vorgehensweise beispielsweise ebenfalls unanwendbar. Überdies sind durch die Anwendbarkeit der JIRL anstatt der DSGVO Friktionen vermeidbar: ansonsten unterfiele die Datenverarbeitung zur Bekämpfung organisierter Kriminalität durch die Gefahrenabwehr- und Strafverfolgungsbehörden der JIRL, während bei der Datenverarbeitung im Zusammenhang mit der Beobachtung organisierter Kriminalität durch die Nachrichtendienste die DSGVO zu beachten wäre. Die in den Übermittlungsnormen erkennbare, enge Kooperation zwischen diesen Behörden unterstreicht gerade die Schlussfolgerung, dass die Verarbeitungen ähnlich sensibel sind.

Auf die Bestandteile der nachrichtendienstlichen Tätigkeit, die nunmehr in den Anwendungsbereich des Unionsrechts fallen, sollte daher grundsätzlich die souveränitätsschonendere JIRL angewandt werden.⁷⁰⁹ Dass die in der Literatur entwickelten einschränkenden Voraussetzungen für das Ziel der Gefahrenabwehr gem. Art. 1 Abs. 1 JIRL (vermutlich) nicht gewahrt werden, ist wegen der Besonderheit nachrichtendienstlicher Tätigkeiten und der mit Gefahrenabwehr- und Strafverfolgung vergleichbaren Sensibilität hinzunehmen.⁷¹⁰ Soweit die Nachrichtendienste allerdings im Einzelfall nicht zum Zweck der Gefahrenabwehr mit potentielltem Straftatbezug oder zur Strafverfolgung handeln, sondern ihre Tätigkeit mit „allgemeiner Gefahrenabwehr“ vergleichbar ist, fällt diese Tätigkeit in den Anwendungsbereich der DSGVO. Wenn der Verfassungsschutz beispielsweise automatisiert Daten verarbeitet, um in Schulen oder anderen Einrichtungen Fortbildungen und Fachtagungen zu Präventionszwecken

⁷⁰⁸ Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 961 Rn. 405, 962 Rn. 409, 412.

⁷⁰⁹ So im Ergebnis auch Wetzling/C. Dietrich, Disproportionate use of commercially and publicly available data, S. 24 f.; Sajfert/Quintel, SSRN Journal 2017, 1, 4: “Therefore, when national intelligence agencies process data for the purposes of the Directive, they should be viewed as competent authorities under Article 2(1) instead of not being covered by EU law”.

⁷¹⁰ Abgesehen davon können die Nachrichtendienste bei den Überlegungen für die einschränkenden Voraussetzungen nicht bedacht worden sein, weil die Überzeugung herrschte, dass das Nachrichtendienstrecht vollständig außerhalb des Anwendungsbereichs des Unionsrechts liege.

anzubieten⁷¹¹, besteht kein potenzieller Straftatbezug und der Anwendungsbereich der DSGVO ist eröffnet.

cc) Vorgaben der JIRL

Soweit der Anwendungsbereich der JIRL eröffnet ist, ist der Gesetzgeber verpflichtet, ihre Normen in nationales Recht umzusetzen. Vor allem in verfahrensrechtlicher Hinsicht sind mit der JIRL weitreichende Änderungen verbunden, auf die materielle Ausgestaltung von Rechtsgrundlagen der Datenverarbeitung hat sie geringere Auswirkungen.⁷¹²

(1) Befugnisse der Aufsichtsbehörde, Art. 47 JIRL

Die JIRL legt fest, dass jeder Mitgliedstaat unabhängige Aufsichtsbehörden zur Überwachung der Richtlinienanwendung etablieren muss, Art. 41 Abs. 1 JIRL. Gem. Art. 47 Abs. 1 JIRL sind alle Aufsichtsbehörden mit „wirksamen Untersuchungsbefugnissen“ auszustatten, hiervon sei „zumindest“ die Befugnis erfasst, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und den zur Aufgabenerfüllung notwendigen Informationen zu erhalten. Darüber hinaus müsse jeder Mitgliedstaat gem. Art. 47 Abs. 2 JIRL vorsehen, dass jede Aufsichtsbehörde über „wirksame Abhilfebefugnisse“ verfüge, „beispielhaft“ seien dies: die Warnung, dass beabsichtigte Verarbeitungsvorgänge gegen die nach der JIRL zu erlassenden Normen verstoßen könnten (lit. a)), die Anweisung, Verarbeitungsvorgänge datenschutzkonform auszugestalten, „insbesondere“ durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder durch Einschränkung der Verarbeitung gem. Art. 16 der Richtlinie (lit. b)), und die Befugnis eine Beschränkung oder sogar ein Verbot der Verarbeitung zu verhängen (lit. c)). Die Mitgliedstaaten müssen ihren Aufsichtsbehörden zudem die Befugnis einräumen, den Justizbehörden Verstöße zur Kenntnis zu bringen und ein gerichtliches Verfahren einleiten oder sich daran beteiligen zu können, Art. 47 Abs. 6 JIRL.

⁷¹¹ Zur Präventionstätigkeit des Landesverfassungsschutzes von Nordrhein-Westfalen, Pfeiffer, Radikalisierungsprävention, 173, 178.

⁷¹² Die JIRL normiert selbst keine Datenerhebungsbefugnisse, sondern setzt ihre Existenz voraus, Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 956 f., Rn. 393 m. Verweis auf BVerfG, Beschluss v. 27.5.2020 – 1 BvR 1873/13 – Rn. 85, die materiellen Vorgaben seien weniger bedeutend, weil die Richtlinie nur auf eine Mindestharmonisierung abzielt, Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 976 Rn. 461; Schenke/Graulich/Ruthig/Schenke/Graulich/Ruthig, Einführung, S. 9 Rn. 33; Möstl/Schwabenbauer/Schröder, Datenschutz-Richtlinie (EU) 2016/680 (JI-RL) Rn. 68 ff.

Wie Art. 47 JIRL unionsrechtskonform auszugestalten ist, ist umstritten. Der Streit wurzelt in der unterschiedlichen Formulierung der Befugnisse der DSGVO im Vergleich zur JIRL: Art. 58 DSGVO zählt die Abhilfebefugnisse der Aufsichtsbehörden abschließend auf, während Art. 47 Abs. 2 JIRL weiter formuliert ist und wirksame Abhilfebefugnisse fordert, die nur beispielhaft aufgezählt sind. Einigkeit herrscht dazu, dass die weite Formulierung Spielräume bei der Umsetzung in nationales Recht bedingt.⁷¹³ Wo diese Regelungsspielräume an ihre Grenzen stoßen, wird hingegen kontrovers beurteilt.

Einerseits werden die Regelungsspielräume so weit verstanden, dass es letztlich bei der im deutschen Datenschutzrecht tradierten (und als schwaches Instrument einzuordnenden⁷¹⁴) Befugnis zur Beanstandung bleibt.⁷¹⁵ Ein mit Anordnungsbefugnissen ausgestatteter Datenschutzkontrolleur sei unvereinbar mit der „Sensibilität und Komplexität der entsprechenden Verarbeitungen und dem Bedürfnis nach ständiger Verfügbarkeit rechtmäßig erhobener Daten und Datenverarbeitungsanlagen“.⁷¹⁶ Wegen der Wechselwirkung mit anderen Befugnissen des Datenschutzbeauftragten, der sich an das Parlament oder die Öffentlichkeit wenden oder entsprechende Bemerkungen in seinen Tätigkeitsbericht aufnehmen könne, um so öffentlichen Druck zu erzeugen, sei die Beanstandung im Ergebnis als „wirksam“ zu beurteilen.⁷¹⁷ Dass die Befugnisse in Art. 47 JIRL „deutlich knapper vorausbestimmt“ würden als in der DSGVO, ermögliche es den Mitgliedstaaten, „ihre JI-Behörden vor der Datenschutzaufsicht besser [zu] schützen“.⁷¹⁸

Dem wird andererseits zu Recht entgegnet, dass Art. 47 Abs. 2 JIRL den Regelungsspielraum der Mitgliedstaaten zumindest insoweit eingrenzt, als sein Wortlaut die Wirksamkeit der Abhilfebefugnisse vorgibt.⁷¹⁹ Wirksam sind die Befugnisse nur, wenn

⁷¹³ Golla, KriPoZ 2019, 238, 243; Bächer, Datenschutzrichtlinie für Polizei und Strafjustiz, 63, 83: „Die Richtlinie belässt den Mitgliedstaaten damit einen beträchtlichen Regelungsspielraum (...)“; Möstl/Schwabenbauer, Hdb. des Polizeirechts, 952, 962 Rn. 412.

⁷¹⁴ Bächer, Datenschutzrichtlinie für Polizei und Strafjustiz 2017, 63, 83; „vergleichsweise milde“, Schulze/Bange, ZD 2019, 199, 201.

⁷¹⁵ § 26 a Abs. 4 S. 3 BVerfSchG i. V. m. § 16 Abs. 2 BDSG; BT-Drs. 18/11325 S. 88; dargestellt in Schenke/Graulich/Ruthig/Siems, § 26 a BVerfSchG Rn. 13.

⁷¹⁶ BT-Drs. 18/11325, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 v. 24.2.2017, S. 88.

⁷¹⁷ Wolff/Brink/Meltzian, § 16 BDSG Rn. 10.

⁷¹⁸ Möstl/Schwabenbauer/Schröder, Datenschutz-Richtlinie (EU) 2016/680 (JI-RL) Rn. 52.

⁷¹⁹ Bächer, Datenschutzrichtlinie für Polizei und Strafjustiz 2017, 63, 83; Golla, KriPoZ 2019, 238, 243; Johannes/Weinhold, Datenschutzrecht bei Polizei und Justiz, S. 59 Rn. 106.

sie verbindlich wirken, der Verantwortliche also daran gebunden ist.⁷²⁰ Dafür sprechen systematische Überlegungen: In der Aufgabennorm, Art. 46 Abs. 1 lit. a JIRL, hat der europäische Gesetzgeber festgelegt, dass die mitgliedstaatliche Aufsichtsbehörde die Umsetzung der Richtlinie „überwacht und durchsetzt“. Eine Aufsichtsbehörde, die Normen durchsetzen soll, ist jedoch darauf angewiesen, dass ihre Abhilfebefugnisse verbindlich sind.⁷²¹ Wo darauf verwiesen wird, dass bindende Anordnungsbefugnisse mit der Sensibilität von Datenverarbeitungen der Strafverfolgungs- und Polizeibehörden nicht vereinbar seien, wird entgegnet, dass die Sensibilität der Datenverarbeitungen es erst recht notwendig erscheinen lasse, rechtswidrige Verarbeitungen zu unterbinden.⁷²² Darüber hinaus wird die ständige Verfügbarkeit rechtmäßiger Daten von Abhilfebefugnissen gegenüber rechtswidrigen Datenverarbeitungen nicht beeinflusst.⁷²³ Richtigerweise muss den Aufsichtsbehörden zumindest das Recht verliehen werden, Weisungen zu erteilen.⁷²⁴

Mitgliedstaatliche Regelungen, die dem nicht gerecht werden, sind unionsrechtswidrig.⁷²⁵

(2) Sonstige Regelungen

Neben den Regelungen zu den Aufsichtsbehörden sind weitere Vorschriften für die Kontrolle der Nachrichtendienste relevant. So sieht Art. 24 JIRL vor, dass der Verantwortliche ein Verzeichnis aller Datenverarbeitungen führt, in dem unter anderem der Zweck der Verarbeitung, die Kategorien betroffener Personen und die Rechtsgrundlagen benannt werden. Dabei handelt es sich um eine Zusammenfassung der wesentlichen Verarbeitungsverfahren in einem „Verarbeitungs-Inhaltsverzeichnis“. ⁷²⁶ Das Verzeichnis muss der Aufsichtsbehörde auf deren Anfrage hin zur Verfügung gestellt werden (Art. 24 Abs. 4). Art. 25 JIRL legt fest, dass die Verwendung automatisierter Datenver-

⁷²⁰ Golla, KriPoZ 2019, 238, 243; schon der Begriff der „Abhilfebefugnis“ setzt voraus, dass die Aufsichtsbehörde bei Verstößen rechtskonforme Zustände herstellen kann, Kühling/Buchner/Bange, Art. 16 BDSG Rn. 29.

⁷²¹ Golla, KriPoZ 2019, 238, 243.

⁷²² Bäcker, Datenschutzrichtlinie für Polizei und Strafjustiz, 63, 84.

⁷²³ Bäcker, Datenschutzrichtlinie für Polizei und Strafjustiz, 63, 84.

⁷²⁴ Golla, KriPoZ 2019, 238, 243; Art. 29-Datenschutzgruppe, Stellungnahme zu einigen grundlegenden Fragestellungen der Richtlinie Justiz/Inneres, EU 2016/680, WP 258, angenommen am 29.11.2017, S. 30; „verbindliche Anordnungen“, Stellungnahme der BfDI ggü. dem BT-Innenausschuss v. 3.3.2017, Ausschuss-Drs. 18(4)788, S. 4.; „direkte Einflussnahmemöglichkeiten“ bei Kühling/Buchner/Bange, Art. 16 BDSG Rn. 29.

⁷²⁵ Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 1155 f. Rn. 1088; Schulze/Bange, ZD 2019, 199, 204; Stellungnahme der BfDI ggü. dem BT-Innenausschuss v. 3.3.2017, Ausschuss-Drs. 18(4)788, S. 3.

⁷²⁶ Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 995 Rn. 543.

arbeitungssysteme mit weitgehenden Protokollierungspflichten verbunden ist. Demnach soll die „Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung“ von Daten auf eine Weise notiert werden, die unter anderem das Datum, die Begründung und die Identität der abrufenden Person erkennen lässt (Art. 25 Abs. 1). Die Protokolle dürfen nur zu eng definierten Zwecken, unter anderem zur Rechtmäßigkeitskontrolle, verwendet werden (Art. 15 Abs. 2) und sind den Aufsichtsbehörden auf Antrag zur Verfügung zu stellen (Art. 15 Abs. 3). Darüber hinaus etablieren die Art. 12 ff. bestimmte Betroffenenrechte: Betroffene müssen über Verarbeitungen ihrer personenbezogenen Daten informiert werden (Art. 12), können von dem Verantwortlichen Bestätigung oder Auskunft über die Datenverarbeitung verlangen (Art. 14) und haben ein Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung (Art. 16). Die beiden erstgenannten Rechte stehen jedoch unter dem Vorbehalt, dass ihre Ausübung unter anderem zum Schutz der nationalen oder öffentlichen Sicherheit beschränkt werden kann (Art. 13 Abs. 3, 15).

b. Anwendbarkeit der DSGVO

Neben der JI-RL ist zum Teil auch die DSGVO anwendbar.

aa) Allgemeine Gefahrenabwehr

Mit der allgemeinen Gefahrenabwehr vergleichbare Tätigkeiten der Nachrichtendienste, wie beispielsweise die Öffentlichkeitsarbeit, fallen in den Anwendungsbereich der DSGVO.

Sollten die „Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten“ bzw. die „Strafvollstreckung“ und „der Schutz und die Abwehr von Gefahren“ gem. Art. 1 Abs. 1 JIRL eng auszulegen und operative Befugnisse notwendig sein, richtet sich zudem die gesamte in den Anwendungsbereich des Unionsrechts fallende Tätigkeit der Nachrichtendienste statt nach der JIRL nach der DSGVO.⁷²⁷

bb) Übermittlung von Privaten an die Nachrichtendienste

Wenn die Mitgliedstaaten Daten selbst erheben, sind sie „nur“ an nationales Recht oder ggf. an sich aus der JIRL ergebende Vorschriften gebunden.⁷²⁸ Wenn sie hingegen Private zur Übermittlung von Daten an die Nachrichtendienste verpflichten, sind diese Privaten an die DSGVO gebunden.⁷²⁹

⁷²⁷ Vgl. [Teil 2 B. II. 2. b. bb\).](#)

⁷²⁸ EuGH C-623/17 v. 6.10.2020 Privacy International Rn. 48.

⁷²⁹ Wolff/Brink/Bäcker, Art. 2 DSGVO Rn. 9c.

Im Anwendungsbereich der ePrivacy-Richtlinie (RL (EU) 2002/58) wurde dies in Bezug auf Telekommunikationsanbieter bereits vom EuGH entschieden: In der Rechtssache *Privacy International* stellte der Gerichtshof fest, dass die Art. 1 Abs. 3 i. V. m. Art. 15 Abs. 1 der RL (EU) 2002/58 so auszulegen sind, dass Übermittlungen von Verkehrs- und Standortdaten an Sicherheitsbehörden sogar in den Anwendungsbereich der Richtlinie fallen, wenn sie zum Schutz der nationalen Sicherheit erfolgen.⁷³⁰ Dasselbe gelte in Bezug auf die gem. Art. 95 DSGVO neben die Richtlinie tretende DSGVO.⁷³¹

Weil zum Schutz der nationalen Sicherheit gem. Art. 4 Abs. 3 EUV nur die Mitgliedstaaten „berufen“ sind, greift auch die Bereichsausnahme in Art. 2 Abs. 2 lit. a) DSGVO nur für staatliche Handlungen.⁷³² Eine Konsequenz daraus ist, dass den datenschutzrechtlichen Aufsichtsbehörden in dieser Konstellation weitreichendere Abhilfebefugnisse zur Verfügung stehen. Gem. Art. 58 Abs. 2 DSGVO können sie gegenüber dem Verantwortlichen (hier den Telekommunikations Providern) unter anderem Verarbeitungsverbote erteilen (lit. f)) oder Geldbußen verhängen (lit. i)) i. V. m. Art. 83 DSGVO.⁷³³ Art. 23 DSGVO ermöglicht Ausnahmeregelungen zum Schutz der nationalen Sicherheit nur für Betroffenenrechte, weshalb die Vorgaben zur aufsichtlichen Kontrolle unabdingbar gelten.

Wie weit die Abhilfebefugnisse gem. Art. 58 Abs. 2 DSGVO im Einzelfall reichen, ist abhängig davon, ob die jeweilige Verarbeitung in den Anwendungsbereich der DSGVO fällt, da die Aufsichtsbehörden die Anwendung der DSGVO „überwachen und durchsetzen“ (Art. 57 Abs. 1 lit. a DSGVO). Da der EuGH in *Privacy International* explizit die „Übermittlung“ dem Anwendungsbereich der Verordnung unterstellt und nicht den Oberbegriff der Datenverarbeitung nutzt⁷³⁴, gelten hierfür die Kontrollbefugnisse nach der DSGVO. Erst die Weiterverarbeitung durch die empfangende Behörde ist von der Kontrollbefugnis nicht mehr erfasst.⁷³⁵

⁷³⁰ EuGH C-623/17 v. 6.10.2020 *Privacy International* Rn. 49.

⁷³¹ EuGH C-623/17 v. 6.10.2020 *Privacy International* Rn. 47. Der EuGH verweist auf die Möglichkeit der Mitgliedstaaten zum Zweck der Strafverfolgung und Gefahrenabwehr (Art. 23 Abs. 1 lit. d)) und für Kontroll-, Überwachungs- und Ordnungsfunktionen, die mit der Ausübung öffentlicher Gewalt verbunden sind, Ausnahmenvorschriften von der DSGVO vorzusehen. Da entsprechende staatliche Tätigkeiten schon gem. Art. 2 Abs. 2 DSGVO vom Anwendungsbereich der DSGVO ausgenommen sind, müssen vergleichbare Tätigkeiten Privater grundsätzlich von der DSGVO erfasst sein, wenn Art. 23 Abs. 1 DSGVO ein Anwendungsbereich zukommen soll.

⁷³² Kühling/Buchner/Bäcker, Art. 23 DSGVO Rn. 16.

⁷³³ Zwar können zum Schutz der nationalen Sicherheit gem. Art. 23 Abs. 1 lit. a DSGVO Ausnahmen etabliert werden, Art. 23 Abs. 1 beschränkt diese Option aber auf bestimmte Vorschriften. Die Art. 51 ff. DSGVO sind davon nicht erfasst.

⁷³⁴ EuGH C-623/17 v. 6.10.2020 *Privacy International* Rn. 49.

⁷³⁵ Kühling/Buchner/Bäcker, Art. 23 DSGVO Rn. 14.

Die Kontrollbefugnis der Aufsichtsbehörde ist jedoch eingeschränkt, denn sie besteht lediglich gegenüber dem Verantwortlichen und erfasst daher nur den Mitwirkungsbeitrag der übermittelnden Provider.

Offen ist, ob die Aufsichtsbehörde gegenüber dem privaten Verantwortlichen tätig werden können, wenn das Übermittlungersuchen rechtswidrig war. Nach der Rechtsprechung des Bundesverwaltungsgerichts handeln die übermittelnden Privaten bei rechtswidrigen Übermittlungersuchen selbst nicht rechtswidrig, weil sie das Übermittlungersuchen inhaltlich gar nicht zu prüfen haben.⁷³⁶ Das bedeutet, die Aufsichtsbehörden könnten ihnen gegenüber auch nicht einschreiten, wenn die nachfolgenden Verarbeitungsschritte Fehler aufweisen oder unzureichend geregelt sind; die Geltung der DSGVO hätte dann keine praktischen Auswirkungen auf die Kontrolle. Andererseits könnte man darauf abstellen, dass die Übermittlungserlaubnis nach der Rechtsprechung des EuGH in *Privacy International* materiell die grundrechtliche Rechtfertigungslast zu tragen hat.⁷³⁷ Wenn das Sekundärrecht aber für die Anwendung der Übermittlungserlaubnis gilt, müsste es eigentlich auch für die Kontrolle der Anwendung gelten. Diese Frage müsste daher unionsrechtlich geklärt werden.

cc) Vorgaben der DSGVO

Die DSGVO stattet die Aufsichtsbehörde mit weitreichenden Befugnissen aus. Gem. Art. 58 Abs. 1 verfügt sie über Untersuchungsbefugnisse und kann verlangen, dass ihr alle zur Aufgabenerfüllung notwendigen Informationen zur Verfügung gestellt werden (lit. a)), dass sie Zugang zu den relevanten personenbezogenen Daten (lit. e)) und Räumlichkeiten des Verantwortlichen oder Auftragsverarbeiters, einschließlich aller Datenverarbeitungsanlagen und -geräte, (lit. f)), erhält. Art. 58 Abs. 2 DSGVO beschreibt die Abhilfebefugnisse, über die die Aufsichtsbehörde im Anwendungsbereich der DSGVO verfügt, abschließend. Demnach kann die Aufsichtsbehörde sogar Verarbeitungsverbote verhängen (lit. f)), die Berichtigung und Löschung personenbezogener Daten verlangen (lit. g)), eine Geldbuße erteilen (lit. i)) oder die Datenübermittlung in Drittländer aussetzen (lit. j)). Wegen ihres zwingenden Charakters sind die Befugnisse der Aufsichtsbehörden nach der DSGVO strukturell weitgehender als die gem. Art. 47 JIRL.

Darüber hinaus etabliert die DSGVO weitreichende Betroffenenrechte (Art. 12 ff.), wie beispielsweise das Recht auf Auskunft über die Verarbeitung oder auf Löschung

⁷³⁶ BVerwG, Urt. v. 30.5.2018 - 6 A 3.16 - Rn. 28.

⁷³⁷ EuGH C-623/17 v. 6.10.2020 *Privacy International* Rn. 47, 49.

personenbezogener Daten. Die Mitgliedstaaten können gem. Art. 23 Abs. 1 jedoch unter anderem zum Schutz der nationalen Sicherheit Ausnahmen von diesen Betroffenenrechten normieren.

3. Unionsgrundrechte

Die Mitgliedstaaten sind bei der „Durchführung“ von Unionsrecht an die Grundrechtecharta gebunden (Art. 52 Abs. 1 S. 1 GRCh).

a. Anwendbarkeit

Der EuGH bejaht die Durchführung von Unionsrecht, wenn dessen Anwendungsbereich in Bezug auf eine Regelung tatsächlich eröffnet ist.⁷³⁸ Ob eine mitgliedstaatliche Handlung ausreichend eng mit dem Anwendungsbereich des Unionsrechts verknüpft ist, richtet sich nach einem Kriterienbündel.⁷³⁹ Wenn das Unionsrecht vollständig determinierenden Charakter hat, erfolgt die grundrechtliche Prüfung ausschließlich am Maßstab der GRCh.⁷⁴⁰ Soweit die vollharmonisierende DSGVO einschlägig ist, sind die Unionsgrundrechte daher zu beachten. Der Anwendungsbereich ist darüber hinaus unter anderem eröffnet, wenn ein Mitgliedstaat in einer Richtlinie vorgesehene Regelungsspielräume in mitgliedstaatliches Recht umsetzt.⁷⁴¹ Soweit im mitgliedstaatlichen Recht Ausnahmen von Betroffenenrechten der JIRL normiert oder die Normen über die Aufsichtsbehörden umgesetzt werden, wird Unionsrecht durchgeführt, sodass die Grundrechtecharta anwendbar ist.⁷⁴² Dies gilt auch, soweit die JIRL im Nachrichtendienstrecht anwendbar ist.⁷⁴³

⁷³⁸ Jarass, Art. 51 GRCh Rn. 24; Callies/Ruffert/Kingreen, Art. 51 GRCh Rn. 7; Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 955 Rn. 387.

⁷³⁹ Bäcker, EuR 2015, 389, 392; Wolff/Brink/Albers, Datenschutzbestimmungen der Polizei- und Nachrichtendienstgesetze des Bundes Rn. 40; Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 955 Rn. 388.

⁷⁴⁰ BVerfG, Beschluss v. 6.11.2019 – 1 BvR 276/17 – Rn. 41 ff.; Wolff/Brink/Albers, Datenschutzbestimmungen der Polizei- und Nachrichtendienstgesetze des Bundes Rn. 40; Callies/Ruffert/Kingreen, Art. 51 GRCh Rn. 11.

⁷⁴¹ Wolff/Brink/Albers, Datenschutzbestimmungen der Polizei- und Nachrichtendienstgesetze des Bundes Rn. 40; Möstl/Schwabenbauer/Schröder, Datenschutz-Richtlinie (EU) 2016/680 (JI-RL) Rn. 61; Jarass, Art. 51 GRCh Rn. 26, 29; Bäcker, EuR 2015, 389, 394 f., 403; Marsch, Europäisches Datenschutzgrundrecht, S. 287.

⁷⁴² Vgl. Müller/Schwabenbauer, Hdb. des Polizeirechts, 952, 957 Rn. 395.

⁷⁴³ In dieser Konstellation prüft das BVerfG grundsätzlich ausschließlich am Maßstab des Grundgesetzes, wobei die Vorgaben aus der GRCh für die Auslegung relevant sind, BVerfG, Beschluss v. 6.11.2019 – 1 BvR 16/13 – Rn. 44 ff., 63 ff, vgl. detailliert Wolff/Brink/Albers, Datenschutzbestimmungen der Polizei- und Nachrichtendienstgesetze des Bundes Rn. 40. Solange die Grundrechte des Grundgesetzes höhere

b. Materielle Vorgaben zur Kontrolle der Nachrichtendienste

Für die Datenverarbeitung der Nachrichtendienste ist vor allem das Datenschutzgrundrecht gem. Artt. 7, 8 GRCh von Bedeutung: Wenn Behörden personenbezogene Daten verarbeiten, greifen sie in den Schutzbereich der Artt. 7, 8 GRCh ein⁷⁴⁴. Art. 8 Abs. 2 S. 2 GRCh verleiht dem Einzelnen das Recht, Auskunft über die Verarbeitung personenbezogener Daten zu erhalten und Berichtigung oder Löschung dieser Daten verlangen zu können. Gem. Art. 8 Abs. 3 GRCh muss die Einhaltung des Datenschutzes von unabhängigen, weisungsfreien⁷⁴⁵ Stellen überwacht werden.⁷⁴⁶ Darüber hinaus kann das Recht auf einen wirksamen Rechtsbehelf gem. Art. 47 GRCh zu beachten sein. Demnach haben Personen, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, bei Gericht einen wirksamen Rechtsbehelf einzulegen (Abs. 1) und können verlangen, dass ihre Sache vor einem unabhängigen, unparteiischen Gericht verhandelt wird (Abs. 2).

aa) Vorratsdatenspeicherung

In den Entscheidungen zur Vorratsdatenspeicherung hat der EuGH Kontrollvorgaben formuliert. So muss bei der Sammlung von Standort- und Verkehrsdaten in Echtzeit eine Vorabkontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle vorgesehen werden, deren Entscheidung bindend ist und die prüft, dass die Datenverarbeitung die Grenzen des „absolut notwendigen“ nicht überschreitet (*Kontrollleur, Distanz, Zeitpunkt und Kontrollergebnisse*). In Eilfällen muss diese Kontrolle „kurzfristig“ nachgeholt werden.⁷⁴⁷

Darüber hinaus ist eine allgemeine und unterschiedslose Vorratsdatenspeicherung zum Schutz der nationalen Sicherheit abhängig davon, dass die „Anordnung Gegenstand einer wirksamen (...) Kontrolle durch ein Gericht oder eine unabhängige Verwal-

Schutzstandards als die vergleichbaren Chartagrundrechte garantieren, sei das „Irritationspotenzial“ allerdings gering, da Art. 53 GRCh ein höheres Schutzniveau nicht ausschließe, *Müller/Schwabenbauer*, Hdb. des Polizeirechts, 952, 958 Rn. 396. Nach Ansicht des EuGH können im nicht determinierten Bereich neben den europäischen Grundrechten mitgliedstaatliche Grundrechte geprüft werden, wenn dadurch „weder das Schutzniveau der Charta, noch der Vorrang, die Einheit und die Wirksamkeit des Unionsrechts beeinträchtigt werden“, *Callies/Ruffert/Kingreen*, Art. 51 GRCh Rn. 10.

⁷⁴⁴ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 169 ff.

⁷⁴⁵ *Marsch*, Europäisches Datenschutzgrundrecht, S. 214 ff.

⁷⁴⁶ Aufgrund des „dürren Wortlauts“ könne man aus Art. 8 Abs. 3 GRCh jedoch „keine konkreten Befugnisse der Datenschutzbehörden“ herleiten, *Marsch*, Europäisches Datenschutzgrundrecht, S. 244 f.

⁷⁴⁷ EuGH C-511/18, C-512/18, C-520/18 v. 6.10.2020 *La Quadrature du Net*, Rn. 189; *European Data Protection Board*, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, S. 12.

tungsstelle“ ist, die unter anderem prüft, ob die „vorzusehenden Bedingungen und Garantien“ eingehalten wurden und deren Entscheidung bindend wirkt.⁷⁴⁸ Da die Kenntnis betroffener Personen notwendige Voraussetzung dafür ist, dass diese ihre Rechte geltend machen können, sei es wichtig, dass Betroffene über die Verarbeitung informiert werden, sobald der Zweck der Maßnahme dadurch nicht mehr gefährdet wird.⁷⁴⁹

bb) Schrems II

Zu den materiellen grundrechtlichen Vorgaben an nachrichtendienstliche Datenverarbeitungen hat sich der EuGH darüber hinaus in der Rechtssache *Schrems II*, im Kontext von Datenverarbeitungen durch amerikanische Nachrichtendienste, geäußert.

(1) Gegenstand der Entscheidung

In dem Vorabentscheidungsersuchen *Schrems II* hatte der EuGH unter anderem zu entscheiden, ob der Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 DSGVO, wonach in den Vereinigten Staaten von Amerika ein angemessenes Schutzniveau für personenbezogene Daten herrscht, das es erlaubt Daten dorthin zu übermitteln, rechtmäßig ergangen ist. Dafür kam es darauf an, ob in den Vereinigten Staaten ein mit der Europäischen Union vergleichbares Datenschutzniveau existiert. Der Beschwerdeführer vor dem nationalen Gericht, Maximilian Schrems, hatte dies in Frage gestellt, weil amerikanische Behörden, wie zum Beispiel das Federal Bureau of Investigation oder die National Security Agency, gegenüber Privatunternehmen wie Facebook Zugang zu personenbezogenen Daten beanspruchen können, ohne dass dafür Beschränkungen gelten oder betroffenen Personen Rechtsbehelfe verliehen werden. Der EuGH prüfte die Vergleichbarkeit des Schutzniveaus unter anderem durch eine Anwendung der einschlägigen Grundrechte (Auslegung der DSGVO-Normen im Lichte der Grundrechte).⁷⁵⁰

(2) Eingriffe in Artt. 7, 8 GRCh

Ob Eingriffe in die Artt. 7, 8 GRCh gerechtfertigt seien, sei abhängig davon, dass in die Verarbeitung eingewilligt wurde oder die Verarbeitung auf einer gesetzlich geregelten legitimen Grundlage erfolgt (Art. 8 Abs. 2 GRCh). Darüber hinaus müsse die gesetzlich

⁷⁴⁸ EuGH C-511/18, C-512/18, C-520/18 vom 6.10.2020 *La Quadrature du Net*, Rn. 168; EuGH C-793/19, C-794/19 v. 20.9.2022 *SpaceNet* und andere, Rn. 72.

⁷⁴⁹ European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, S. 13.

⁷⁵⁰ EuGH C-311/18 v. 16.7.2020 *Schrems II* Rn. 55, 60 ff., 168 ff., 199.

vorgesehene Einschränkung den Wesensgehalt dieser Rechte achten, nach dem Grundsatz der Verhältnismäßigkeit erforderlich sein und tatsächlich Gemeinwohlinteressen oder Rechte anderer dienen (Art. 52 Abs. 1 GRCh). Um verhältnismäßig zu sein und Beschränkungen von Artt. 7, 8 GRCh auf das „absolut Notwendige beschränken“ zu können, müsse die Rechtsgrundlage „klare und präzise Regeln für die Tragweite und Anwendung der betreffenden Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen.“ Die Umstände sowie die Voraussetzung einer Maßnahme zur Datenverarbeitung müssten in der Rechtsgrundlage festgelegt werden.⁷⁵¹

Bei der Subsumtion der maßgeblichen Rechtsgrundlagen⁷⁵² unter diese Vorgaben geht der EuGH auf drei Aspekte ein: Erstens prüft er, ob die Rechtsgrundlage ausreichende Einschränkungen vorsieht, zweitens, ob Betroffenen gerichtlich durchsetzbare Rechte verliehen werden und drittens, ob Sammelerhebungen verhältnismäßig sind.⁷⁵³

Zum ersten Aspekt zitiert der EuGH zunächst den DSS-Beschluss der Kommission, wonach der Foreign Intelligence Surveillance Court (FISC) keine individuellen Überwachungsmaßnahmen, sondern lediglich abstrakte Überwachungsprogramme prüfe. Der FISC kontrolliere, „ob diese Überwachungsprogramme dem Ziel entsprechen, Auslandsaufklärungsdaten zu erlangen“, nicht jedoch, ob Betroffene „vorschriftsgemäß als Zielpersonen für die Beschaffung von Aufklärungsdaten ausgewählt wurden“.⁷⁵⁴

„Demzufolge“ ergebe sich aus der Rechtsgrundlage nicht, dass zur Durchführung von Programmen zur Auslandsaufklärung „Einschränkungen“ bestünden oder für potentiell Betroffene Nicht-US-Personen „Garantien“ existierten.⁷⁵⁵ Im Umkehrschluss

⁷⁵¹ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 173-176.

⁷⁵² Ein detailliertes Verständnis der Rechtsgrundlagen ist wegen der knappen Auseinandersetzung des EuGH damit in dem hier relevanten Abschnitt des Urteils zu Artt. 7, 8, 47 GRCh nicht erforderlich. Section 702 FISA erlaubt es amerikanischen Behörden, Personen zu überwachen, die keine US-Bürger sind und sich außerhalb des amerikanischen Staatsgebiets aufhalten. Auf dieser Rechtsgrundlage sind amerikanische Behörden berechtigt, private Anbieter zu verpflichten, ihnen die gesamte Kommunikation von Selektoren offenzulegen (PRISM-Programm). Auf Section 702 FISA basiert auch das UPSTREAM-Programm, wonach US-Behörden die Internetprovider verpflichten können, zu dulden, dass die Behörde Datenflüsse (Meta- und Inhaltsdaten) kopiert und nach Selektoren filtert, die sich im Ausland befindende Nicht-Staatsbürger betreffen. Die zweite relevante „Rechtsgrundlage“ ist die E.O. 12333, ein Exekutivbeschluss des Präsidenten, wonach sich Behörden Zugang zu über Seekabel transportierten Daten verschaffen können, bevor diese das amerikanische Festland erreichen. Gemäß der Presidential Directive PPD-28 müssen solche nachrichtendienstlichen Tätigkeiten „so gezielt wie möglich“ erfolgen, vgl. im Detail EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 60 ff.

⁷⁵³ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 179 ff., 181 ff., 183.

⁷⁵⁴ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 179.

⁷⁵⁵ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 180.

heißt das, dass eine solche nachrichtendienstliche Datenverarbeitung nur dann verhältnismäßig ist, wenn eine Genehmigung durch den FISC vorliegt, die sich darauf bezieht, dass die konkrete Zielperson⁷⁵⁶ vorschriftsgemäß ausgewählt wurde oder der FISC diese konkrete Auswahl nachträglich kontrolliert. Ob der EuGH eine Vorabgenehmigung oder eine nachträgliche Aufsicht fordert, kann wegen der zweideutigen Formulierung nicht abschließend festgestellt werden.⁷⁵⁷ Jedenfalls aber fordert das Gericht eine unabhängige Kontrolle konkreter Zielpersonen bzw. Selektoren (*Kontrolleur, Distanz, Kontrollergebnisfolgen*).

Zweitens würden der betroffenen Person insgesamt keine Rechte verliehen, die gegenüber amerikanischen Behörden gerichtlich durchsetzbar sind.⁷⁵⁸ Soweit Sammelerhebungen einer großen Menge signalerfassender Aufklärungsdaten ermöglicht würden, bestünde drittens „keine hinreichend klare und präzise Eingrenzung des Umfangs einer solchen Sammelerhebung“. ⁷⁵⁹ Insgesamt würden die Rechtsgrundlagen den aus dem Verhältnismäßigkeitsgrundsatz folgenden Mindestanforderungen nicht gerecht, weshalb die auf diesen Normen basierenden Überwachungsmaßnahmen nicht auf „das zwingend erforderliche Maß begrenzt“ seien.⁷⁶⁰

(3) Eingriffe in Art. 47 GRCh

Wenn Betroffenen kein Rechtsmittel verliehen wird, mit dem sie Zugang zu den sie betreffenden personenbezogenen Daten erlangen oder eine Berichtigung oder Löschung dieser Daten verlangen können, ist der Wesensgehalt von Art. 47 GRCh verletzt. Es sei dem Rechtsstaat „inhärent, dass eine wirksame, zur Gewährleistung der Einhaltung des Unionsrechts dienende gerichtliche Kontrolle vorhanden sein muss.“⁷⁶¹

Die Europäische Kommission habe in ihrem Angemessenheitsbeschluss zwar festgestellt, dass „einige“ Rechtsgrundlagen amerikanischer Nachrichtendienste keinen Rechtsbehelf vorsehen, sei jedoch zu dem Schluss gekommen, dass die Einsetzung einer von den Nachrichtendiensten unabhängigen Ombudsperson dieses Manko kompensieren könne. Demgegenüber stellt der EuGH in Frage, ob die Ombudsperson tatsächlich unabhängig von der Exekutive ist. Zudem verfüge die Ombudsperson nicht über

⁷⁵⁶ Übertragen auf die deutsche Rechtslage müsste man hier von Selektoren sprechen, die nicht zwingend personenbezogen sein müssen.

⁷⁵⁷ Das EDPB interpretiert diese Passage als Vorgabe zu einer nachträglichen „independent oversight“ der Umsetzung, European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, S. 12 Rn. 40. Der Begriff „autorisiert“ in Rn. 179 des Urteils spricht hingegen eher für das Erfordernis einer Vorab-Genehmigung.

⁷⁵⁸ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 181 f.

⁷⁵⁹ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 183.

⁷⁶⁰ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 184 f.

⁷⁶¹ EuGH C-311/18 v. 16.7.2020 Schrems II Rn. 187 m. w. N.

verbindlichen Entscheidungsbefugnisse gegenüber den Nachrichtendiensten. Der Anerkennungsbeschluss der Kommission verleihe Betroffenen auch keine gesetzlichen Garantien, auf die sie sich berufen könnten. Im Ergebnis sei der Ombudsmechanismus mit dem in Art. 47 GRCh garantierten Rechtsweg daher nicht vergleichbar (*Kontrollleur und Distanz*).⁷⁶²

(4) Verallgemeinerbare Aussagen?

Ob diese Maßstäbe des EUGH über den Einzelfall hinaus als grundrechtliche Vorgaben an nachrichtendienstliche Verarbeitungen gelten, ist offen. Insgesamt hat der EuGH der inhaltlichen Prüfung der Artt. 7, 8, 47 GRCh nur vergleichbar wenige Randnummern gewidmet. Seine Ausführungen zu den grundrechtlichen Standards nachrichtendienstlicher Tätigkeiten sind „vage“.⁷⁶³ Teilweise zitiert der EuGH den Anerkennungsbeschluss der Europäischen Kommission und ergänzt anschließend, dass der beschriebene Sachverhalt die Voraussetzungen der Artt. 7, 8 GRCh nicht erfülle. Dann ergibt sich daraus nur eine grundrechtliche Vorgabe, wenn man einen Umkehrschluss zieht. Obwohl der EuGH vage formuliert, kommt er zu dem (folgenreichen) Ergebnis, dass die Rechtsgrundlagen unverhältnismäßig sind. Wenn es sich bei den bemängelten Aspekten nicht um verbindliche grundrechtliche Vorgaben handelte, ließe sich daraus jedoch keine Unverhältnismäßigkeit ableiten. Für die Rechtskontrolle der Nachrichtendienste ergibt sich aus *Schrems II* daher, dass sie nur grundrechtskonform ausgestaltet ist, wenn eine auf die konkrete Zielperson (oder den konkreten Selektor) bezogene Vorab-Genehmigung oder Aufsicht einer unabhängigen Stelle gegeben ist und Betroffene über Rechtsbehelfe verfügen, auf deren Grundlage sie vor einem unabhängigen Organ⁷⁶⁴ die Auskunft über die Verarbeitung sowie die Löschung oder Berichtigung ihrer personenbezogenen Daten verlangen können.⁷⁶⁵ Für dieses Ergebnis spricht, dass der EGMR bezogen auf Art. 8 EMRK, der bei der Auslegung der Grundrechte-

⁷⁶² EuGH C-311/18 v. 16.7.2020 *Schrems II* Rn. 195- 197.

⁷⁶³ *Bignami*, Verfassungsblog vom 29.7.2020.

⁷⁶⁴ EuGH C-311/18 vom 16.7.2020 *Schrems II* Rn. 197; European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, S. 14 Rn. 47.

⁷⁶⁵ Vgl. *Bignami*, Verfassungsblog vom 29.7.2020: „On this, it is clear from *Schrems II* that independent courts should have oversight and remedial powers [...]“; *European Data Protection Board*, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, S. 12 ff.

Charta gem. Art. 52 Abs. 3 GRCh als Mindestschutzstandard zu beachten ist⁷⁶⁶, ebenfalls eine unabhängige Genehmigung oder Aufsicht und ein nachträgliches Rechtsmittel fordert.⁷⁶⁷

cc) Art. 52 Abs. 3 GRCh i. V. m. Art. 8 EMRK

Insgesamt ist die Rechtsprechung des EuGH zu den Vorgaben an die grundrechtskonforme Tätigkeit der Nachrichtendienste und damit zur unionsrechtskonformen Ausgestaltung der Rechtskontrolle dieser Tätigkeiten (noch) begrenzt. Für die weitere Ausdifferenzierung der Rechtsprechung wird sich der EuGH auch mit der – im Vergleich detaillierten – Rechtsprechung des EGMR⁷⁶⁸ auseinandersetzen müssen, die auf der Grundlage von Art. 52 Abs. 3 GRCh für die Auslegung von Artt. 7, 8 GRCh von Bedeutung ist.

4. Fazit: Mindestens teilweise Anwendbarkeit des Unionsrechts

Der EuGH hat in den letzten Jahren zwei unterschiedliche Definitionen zum Begriff der nationalen Sicherheit eingeführt, die Auswirkungen auf die Subsumtion der nachrichtendienstlichen Tätigkeit haben. Hier bleibt die weitere Rechtsprechung abzuwarten.

Wendet man die ausführliche Definition des EuGH zur nationalen Sicherheit auf die Nachrichtendienste an, ergibt sich ein differenziertes Bild: teilweise fallen die Tätigkeiten in den Anwendungsbereich des Unionsrechts, teilweise nicht.⁷⁶⁹ Die Subsumtion ist an dieser Stelle (noch) mit großen Unsicherheiten behaftet, weil nicht eindeutig ist, mit welcher Intention der EuGH den Begriff „unmittelbar“ genutzt hat. Soweit das Unionsrecht eröffnet ist, fallen die meisten nachrichtendienstlichen Tätigkeiten in den Anwendungsbereich der JIRL und manche in den der DSGVO. Die Zuordnung ist erstens abhängig davon, ob die Nachrichtendienste mit dem Auftrag der Gefahrenabwehr betraut sind – oder nicht. Zweitens ist entscheidend, ob Art. 1 Abs. 1 JIRL so eng auszulegen ist, dass nur operativ tätig werdende Behörden davon erfasst sind.

Dass als Folge der Anwendung der ausführlichen Definition des EuGH das Unionsrecht einerseits gar nicht einschlägig ist, andererseits jedoch die JIRL und am Rande die

⁷⁶⁶ Jarass, Art. 52 GRCh Rn. 62 ff.; European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, S. 4, 6, 12 ff.; Johannes/Weinhold, Datenschutzrecht bei Polizei und Justiz, S. 36 Rn. 31.

⁷⁶⁷ Zu einem ähnlichen Ergebnis kommt auch das EDPD, vgl. European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, S. 12.

⁷⁶⁸ Vgl. [Teil 2 B. I. 4.](#)

⁷⁶⁹ Vgl. [Teil 2 B. II. 1. c.](#)

DSGVO anzuwenden sind, stellt den Gesetzgeber vor eine komplizierte Aufgabe. In Bezug auf die externe Rechtskontrolle der Nachrichtendienste besteht eine denkbare, unionsrechtskonforme Lösungsoption darin, die Befugnisse der Datenschutzaufsicht generell an Art. 47 JIRL (oder Art. 58 DSGVO) zu orientieren, auch dort, wo sie nicht anwendbar sind. Dies gilt auch für den UKRat und die G 10-Kommissionen, soweit sie als laufende Datenschutzkontrolleure agieren.⁷⁷⁰

Soweit europäisches Sekundärrecht anwendbar ist, ist darüber hinaus die GRCh zu beachten. Insbesondere die Artt. 7, 8, 47 GRCh sind für nachrichtendienstliche Datenverarbeitungen von Bedeutung. Aus der bisher knappen Rechtsprechung des EuGH zu Datenverarbeitungen im Nachrichtendienstrecht folgt, dass jedenfalls manche Datenverarbeitungen der Kontrolle durch eine unabhängige Institution bedürfen, um verhältnismäßig zu sein und dass Betroffene grundsätzlich über Datenverarbeitungen zu informieren sind, da sie ein Recht darauf haben, sich gerichtlich dagegen zur Wehr setzen zu können. Dass die Tätigkeiten mitgliedstaatlicher Nachrichtendienste im Ergebnis an europäischen Grundrechten zu messen sind, ist vor dem Hintergrund, dass der EuGH in *Schrems II* sogar die Handlungen amerikanischer Nachrichtendienste an europäischen Grundrechten gemessen hat, nur folgerichtig.⁷⁷¹

⁷⁷⁰ Da diesen beiden Kontrolleuren anders als den LfDI und dem BfDI aber wirksame Abhilfebefugnisse zur Verfügung stehen, wären die Voraussetzungen von Art. 47 Abs. 1 JIRL erfüllt (vgl. [Teil 3 D. 6.](#)).

⁷⁷¹ Insoweit wurde die bisher herrschende Meinung, dass europäische Nachrichtendienste wegen Art. 4 Abs. 2 S. 3 EUV nicht an Unionsrecht gebunden sind, als „hypocrisy“ bezeichnet, vgl. statt vieler besonders deutlich *Baker, Lawfare* 2021.

Teil 3

Vereinbarkeit des einfachen Rechts mit höherrangigen Vorgaben

Inwieweit das Kontrolldesign im Bundes- und Landesrecht den verfassungs-, konventions- und unionsrechtlichen Vorgaben entspricht, wird im Folgenden dargestellt. Dazu wird zunächst ausgeführt, inwieweit die Gesetze bereits unabhängige Vorabkontrollen vorsehen (A.). Darauf folgt eine Analyse der bundesweit siebzehn Regelungswerke für die Tätigkeit der G 10-Kommissionen (B.). Anschließend werden das Kontrolldesign des UKRats (C.) und die Rechtsgrundlagen für die Kontrolle der Datenschutzbeauftragten (D.) erörtert. Sodann werden die Defizite der Kernbereichsschutzkonzepte diskutiert (E.), bevor abschließend dargestellt wird, inwieweit bereits *de lege lata* ein Kontroll-Gesamtüberblick existiert (F.). Die Defizite des einfachen Rechts werden sodann gesammelt präsentiert (F.).

A. Vorabkontrollen bei eingriffsintensiven Maßnahmen

Spätestens seit der Verfassungsgerichtsentscheidung zum bayerischen Verfassungsschutzgesetz vom 26. April 2022¹ steht fest, dass für alle eingriffsintensiven nachrichtendienstliche Befugnisse unabhängige Vorabkontrollen einzuführen sind².

I. Vorabkontrollen de lege lata

Um feststellen zu können, für welche eingriffsintensiven Maßnahmen in verfassungswidriger Weise bisher noch keine unabhängige Vorabkontrolle etabliert wurde, muss zunächst untersucht werden, inwieweit bereits unabhängige Vorabkontrollen vorgeschrieben sind. Teilweise waren unabhängige Vorabkontrollen auch außerhalb von

¹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17.

² Vgl. [Teil 2 A. III. 3. d. aa.](#)

Eingriffen in Art. 10 Abs. 1 GG bereits geltendes Recht, bevor das Bundesverfassungsgericht sie in der Entscheidung zum bayerischen Verfassungsschutzgesetz³ für besonders eingriffsintensive Befugnisse zwingend vorgeschrieben hat. Es gibt Genehmigungsvorbehalte zugunsten von Gerichten (a)), der G 10-Kommissionen (b)) oder des UKRats (c)).

1. Richtervorbehalt

Teilweise werden Gerichte mit der Vorabkontrolle betraut.

a. Wohnraumüberwachung

Dies betrifft zunächst die Befugnisse zur Wohnraumüberwachung, die wegen Art. 13 Abs. 4 GG nur angewandt werden dürfen, wenn zuvor eine richterliche Genehmigung erteilt wurde. Die dazu ermächtigenden Nachrichtendienstgesetze⁴ normieren, dass eine richterliche Anordnung erfolgen muss.⁵

b. Sonstige Befugnisse

In Bayern gilt der Richtervorbehalt neben der Wohnraumüberwachung auch für die Online-Durchsuchung (Art. 11 Abs. 1 i. V. m. Art. 9, 10 BayVSG), für bestimmte Formen des Einsatzes Verdeckter Mitarbeiter (Art. 18 Abs. 4 N.2 BayVSG), für Vertrauensleute (Art. 19 Abs. 1 S. 2 BayVSG) sowie für längerfristige Observationen (Art. 19a Abs. 2 S. 1 Nr. 2 BayVSG).

In Hessen stehen der Einsatz von IMSI-Catchern zur Standortermittlung (§ 9 Abs. 1 HVSG), längerfristige Observationen (§ 11 Abs. 2, 4 HVSG) und der Einsatz von verdeckten Mitarbeitern und Vertrauensleuten (§§ 12, 13 Abs. 1 HVSG) unter einem richterlichen Genehmigungsvorbehalt.

In Sachsen muss ein Einsatz von verdeckten Mitarbeitern und Vertrauensleuten, der über ein Jahr andauert oder gezielt gegen bestimmte Personen bzw. in zu privaten Wohnzwecken genutzten Räumlichkeiten eingesetzt wird, richterlich genehmigt werden (§ 11 Abs. 5 S. 1 Nr. 2, Abs. 1 S. 2 SächsVSG, § 12 Abs. 1 i. V. m. § 11 Abs. 5 SächsVSG). Außerdem müssen bestimmte Observationen (§ 13 Abs. 3 Nr. 2 SächsVSG) und der

³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17.

⁴ Vgl. [Teil 1 B. III. 1. i.](#)

⁵ § 9 Abs. 4 BVerfSchG; § 5 BNDG, §§ 9 Abs. 4 BVerfSchG; § 5 Abs. 1 Hs. 2 MADG, §§ 9 Abs. 4 BVerfSchG; Art. 9, 11 Abs. 1 [BayVSG](#); § 6 Abs. 1 S. 3 ff. [BWLVS](#); § 18 Abs. 4 [LVerfSchG RP](#); §§ 7, 8 Abs. 1 S. 1 ff. [HVSG](#); § 8 Abs. 4 [HmbVerfSchG](#); § 9 Abs. 1 S. 4 [VSG Bln](#); § 11 Abs. 2 S. 3 ff. [ThürVerfSchG](#); § 8 Abs. 2 S. 3 ff. [VerfSchG LSA](#); § 10 Abs. 1 [SächsVSG](#); § 8 Abs. 5 [SVerfSchG](#).

Einsatz von IMSI-Catchern, der durchgehend länger als vier Wochen andauert, richterlich angeordnet werden (§ 14 Abs. 3 S. 1, Abs. 2 SächsVSG).

2. Genehmigungsvorbehalte zugunsten der G 10-Kommission

Der klassische Auftrag der G 10-Kommissionen besteht darin, Beschränkungen nach dem G 10 zu kontrollieren.⁶ Darüber hinaus wurden jedoch weitere nachrichtendienstliche Befugnisse mit einem Genehmigungsvorbehalt zugunsten der G 10-Kommission verbunden.

a. Auskunftersuchen

Einige Fachgesetze sehen vor, dass der Nachrichtendienst eine Auskunft über personenbezogene Daten von Privatunternehmen nur verlangen kann, wenn die G 10-Kommission dies genehmigt hat. Der Prüfauftrag der G 10-Kommission ist parallel zum Prüfauftrag bei Beschränkungen nach dem G 10 formuliert, sie soll die „Zulässigkeit“ und „Notwendigkeit“ prüfen.⁷

Alle 17 Gesetze, die zur Einholung von Verkehrsdaten bei Telekommunikationsanbietern berechtigen, normieren eine unabhängige Vorabkontrolle durch die G 10-Kommission.⁸ Diese Ausgestaltung entspricht derjenigen für die Abfrage von Nutzungsdaten bei Telemedienanbietern.⁹ Von den achtzehn Gesetzen, die festlegen, dass der Nachrichtendienst Bestandsdaten nach dem TKG abfragen kann, enthalten

⁶ Vgl. [Teil 3 B. II.](#)

⁷ Definition s.u. [Teil 3 B. II. 1.](#) Gem. § 26 a Abs. 1 S. 3 [LVerfSchG SH](#) ist die G 10-Kommission „zu beteiligen“. Aus [LT-Drs. SH 18/713](#), Entwurf eines Gesetzes zur Änderung des Landesverwaltungsgesetzes und des Landesverfassungsschutzgesetzes - Anpassung des manuellen Abrufs der Bestandsdaten nach dem Telekommunikationsgesetz an die verfassungsrechtlichen Vorgaben v. 4.10.2013, S. 16 f. könnte man schließen, dass damit nur eine „Unterrichtung“ gemeint ist, eine Entscheidung also gerade nicht getroffen wird. Dass dies auch praktisch so gehandhabt wird, wurde von der Geschäftsführung der G 10-Kommission auf Nachfrage bestätigt.

⁸ § 8b Abs. 2, 10 BVerfSchG; § 4 BNDG, § 8b Abs. 2 BVerfSchG; § 4 Abs. 1 MADG, § 8 Abs. 2 BVerfSchG; Art. 17 Abs. 3 S. 1, Art. 15 Abs. 2 [BayVSG](#), Art. 2 AGG10BY; §§ 5b Abs. 1, § 5 Abs. 2 Nr. 14, § 7c Abs. 2 [VSG NRW](#); § 5b Abs. 6 [BWLVS](#); § 10 Abs. 5 [HVSG](#); § 13 Abs. 7 [LVerfSchG RP](#); § 21 Abs. 3 S. 2 [NVerfSchG](#); §§ 7a Abs. 2, § 7 Abs. 3 Nr. 4 [HmbVerfSchG](#), § 1 Abs. 3 HmbG10AusfG; § 8a Abs. 7, § 8b Abs. 2, § 26a Abs. 1 S. 3 [LVerfSchG SH](#); § 24a Abs. 4, 1 Nr. 4 VerfSchG MV; § 14a Abs. 5, Abs. 4 Nr. 2 [BbgVerfSchG](#); § 27a Abs. 5 S. 1, 6 [VSG Bln](#); § 16 Abs. 2 [SächsVSG](#); § 8 Abs. 4 S. 4 [ThürVerfSchG](#); § 17a Abs. 5 S. 3 VerfSchG LSA.

⁹ Vgl. Fn. 8 für die Fundstellen. Davon abweichend nur: § 7a Abs. 2, § 7 Abs. 3 S. 1 Nr. 5 [HmbVerfSchG](#), § 1 Abs. 3 [HmbG10AusfG](#); § 24a Abs. 4, 1 Nr. 5 [VerfSchG MV](#); § 14a Abs. 5, Abs. 4 Nr. 3 [BbgVerfSchG](#).

nur sieben einen Vorbehalt der Vorabkontrolle durch die G 10-Kommission.¹⁰ 17 Nachrichtendienstgesetze ermächtigen zur Abfrage von Fluggastdaten bei Flugunternehmen sowie Computerreservierungs- und Distributionsunternehmen, wobei elf von ihnen die Ausübung dieser Befugnis von einer unabhängigen Vorabkontrolle durch die G 10-Kommission abhängig machen.¹¹ Während insgesamt 17 Gesetze eine Kontodatenabfrage normieren, ordnen nur elf eine Vorabkontrolle an.¹² Alle zehn Gesetze, die zu Auskünften bei Postdienstleistern berechtigen, sehen eine Genehmigungspflicht vor.¹³

¹⁰ Teilweise wird die Kommission generell dazu ermächtigt, die Zulässigkeit und Notwendigkeit zu prüfen (§ 10 Abs. 5 [HVSG](#), § 17a Abs. 5 S. 3 [VerfSchG-LSA](#), § 14a Abs. 5 [BbgVerfSchG](#), §§ 8a Abs. 7, 8b Abs. 2, § 26a Abs. 1 S. 3 [LVerfSchG SH](#); § 17 Abs. 3, § 16 Abs. 2 [SächsVSG](#)), teilweise soll sie nur die Abfrage bei besonderen Bestandsdaten, „mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird“ genehmigen oder eingesetzt werden, wenn die Abfrage anhand von „einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt“ wird (§ 21 Abs. 3 S. 2 [NVerfSchG](#), § 11a Abs. 7, §§ 15b Abs. 3, Abs. 1 S. 2, § 15a Abs. 2 [SVerfSchG](#)). Bezüglich der saarländischen Regelung muss jedoch darauf hingewiesen werden, dass § 15b Abs. 3 nur auf § 15a Abs. 1 [SVerfSchG](#) verweist, der die Unterrichtung der Kommission vorschreibt, hingegen nicht auf § 15a Abs. 2 [SVerfSchG](#), der die Kommission mit der Prüfung der Zulässigkeit und Notwendigkeit beauftragt. Die Normen sind teilweise veraltet, da die Verweise auf das zwischenzeitlich novellierte TKG noch nicht angepasst wurden.

¹¹ § 8a Abs. 1 Nr. 1 BVerfSchG; § 3 BNDG, § 8a Abs. 1 Nr. 1 BVerfSchG; § 4a MADG, § 8a Abs. 1 Nr. 1 BVerfSchG; Art. 17 Abs. 3 S. 1, Art. 16 Abs. 1 [BayVSG](#), Art. 2 AGG10BY; § 5b Abs. 6 [BWLVS](#); § 13 Abs. 7 [LVerfSchG RP](#); § 21 Abs. 3 S. 2 [NVerfSchG](#); § 7a Abs. 2, § 7 Abs. 3 S. 1 Nr. 1 [HmbVerfSchG](#), § 1 Abs. 3 [HmbG10AusfG](#); § 27a Abs. 5 S. 1, 6 [VSG Bln](#); § 16 Abs. 2 [SächsVSG](#); § 8 Abs. 4 S. 4 [ThürVerfSchG](#). Eine Befassung der G 10-Kommission ist in Bayern, Hessen, Schleswig-Holstein, Brandenburg, Mecklenburg-Vorpommern und Sachsen-Anhalt nicht vorgesehen. Die [VSG NRW](#), [BremVerfSchG](#) und [SVerfSchG](#) enthalten keine solche Befugnis.

¹² § 8b Abs. 2 BVerfSchG; § 3 BNDG, § 8b Abs. 2 BVerfSchG; § 4a Abs. 1 MADG, § 8b Abs. 2 BVerfSchG; §§ 5b Abs. 1, § 5 Abs. 2 Nr. 13, § 7c Abs. 1 [VSG NRW](#); § 5b Abs. 6 [BWLVS](#); § 13 Abs. 7 [LVerfSchG RP](#); § 21 Abs. 3 S. 2 [NVerfSchG](#); §§ 7a Abs. 2, § 7 Abs. 3 S. 1 Nr. 2 [HmbVerfSchG](#), § 1 Abs. 3 [HmbG10AusfG](#); § 27a Abs. 5 S. 1, 6 [VSG Bln](#); § 16 Abs. 2 [SächsVSG](#); § 8 Abs. 4 S. 4 [ThürVerfSchG](#). Eine Befassung der G 10-Kommission ist in Bayern, Hessen, Schleswig-Holstein, Brandenburg, Mecklenburg-Vorpommern und Sachsen-Anhalt nicht vorgesehen. Die [BremVerfSchG](#) und [SVerfSchG](#) enthalten keine solche Befugnis.

¹³ Art. 17 Abs. 3 S. 1, Art. 15 Abs. 2 [BayVSG](#), Art. 2 AGG10BY; § 5b Abs. 6 [BWLVS](#); § 13 Abs. 7 [LVerfSchG RP](#); die Genehmigungspflicht besteht aber nur hinsichtlich „sonstiger Auskünfte zu den Umständen des Postverkehrs“, nicht bei der Auskunft über Bestandsdaten, § 10 Abs. 5, Abs. 4 Nr. 1 [HVSG](#); §§ 5b Abs. 1, § 5 Abs. 2 Nr. 10 [VSG NRW](#); §§ 8a Abs. 7, § 8b Abs. 2, § 26a Abs. 1 S. 3 [LVerfSchG SH](#); § 24a Abs. 4, 1 Nr. 3 [VerfSchG MV](#); § 14a Abs. 5, Abs. 4 Nr. 1 [BbgVerfSchG](#); § 27a Abs. 5 S. 1, 6 [VSG Bln](#); § 17a Abs. 5 S. 3 [VerfSchG LSA](#).

b. Ton- und Bildaufzeichnungen außerhalb von Wohnungen

In vier Bundesländern entscheidet die G 10-Kommission über die Übertragung bzw. Aufzeichnung des nicht öffentlich gesprochenen Wortes.¹⁴ In Niedersachsen ist zudem eine Vorabkontrolle für verdeckte Bildübertragungen und -aufzeichnungen erforderlich (§§ 21 Abs. 3, 14 Abs. 1 Nr. 8 NVerfSchG.).

c. IMSI/IMEI-Catcher

Gem. elf der 16 Gesetze, die den Einsatz technischer Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes oder zur Ermittlung der Geräte- oder Kartennummer ermöglichen, muss die G 10-Kommission grundsätzlich vorab über die Zulässigkeit und Notwendigkeit der Maßnahme entscheiden.¹⁵ Die niedersächsische Regelung sieht darüber hinaus vor, dass die G 10-Kommission über „Verlängerungen“ der Maßnahme zu entscheiden habe.¹⁶ Die Norm des saarländischen Verfassungsschutzgesetzes ordnet in diesem Zusammenhang nur an, dass die Kommission zu unterrichten ist (§ 8 Abs. 7 i.V.m. § 15a Abs. 1 SVerfSchG). Allerdings verweist § 8 Abs. 7 SVerfSchG gerade nicht auf den Absatz von § 15a SVerfSchG, in dem geregelt ist, dass die G 10-Kommission über die Zulässigkeit und Notwendigkeit entscheidet (§ 15a Abs. 2 SVerfSchG).

In Brandenburg und Thüringen ist die Anwendung der Befugnis nicht mit einem Genehmigungsvorbehalt verbunden. In Hessen wiederum ist das Amtsgericht am Dienort des Landesamts für Verfassungsschutz für die Genehmigung zuständig¹⁷.

¹⁴ § 5b Abs. 1, § 5 Abs. 2 Nr. 6 [VSG NRW](#); §§ 17 Abs. 2, 14 Abs. 2 [LVerfSchG RP](#), § 2 Abs. 1 [AG G 10 RP](#); §§ 21 Abs. 3, § 14 Abs. 1 Nr. 10 [NVerfSchG](#); § 10 Abs. 1 Nr. 7, Abs. 6 [VerfSchG MV](#).

¹⁵ §§ 9 Abs. 4, § 8b Abs. 2 BVerfSchG; § 5 BNDG, § 9 Abs. 4, § 8b Abs. 2 BVerfSchG; §§ 5b Abs. 1, § 5 Abs. 2 Nr. 12, § 7b [VSG NRW](#); § 6 Abs. 2 S. 5, § 5b Abs. 6 [BWLVS](#); §§ 15, § 14 Abs. 2 S. 4 [LVerfSchG RP](#), § 2 Abs. 1 [AG G 10 RP](#); §§ 14 Abs. 1 Nr. 11, 15, 19, § 21 Abs. 3 [NVerfSchG](#); § 8 Abs. 10 S. 6, § 7a Abs. 1 [HmbVerfSchG](#), § 1 Abs. 3 [HmbG10AusfG](#); § 10 Abs. 7 S. 7, § 24a Abs. 4 [VerfSchG MV](#); §§ 17a Abs. 6 S. 5, Abs. 5 [VerfSchG-LSA](#), §§ 8a Abs. 7, § 8b Abs. 2, § 26a Abs. 1 S. 3 [LVerfSchG SH](#) wird laut der Geschäftsführung der G 10-Kommission so ausgelegt, dass die Kommission nicht formal zustimmen muss, sondern nur informiert wird. Diese Praxis müsste geändert werden, um ein verfassungskonformes Kontrolldesign realisieren zu können.

¹⁶ §§ 14 Abs. 1 Nr. 11, 15, 19, 21 Abs. 3 [NVerfSchG](#): „Anordnungen und Verlängerungen des Einsatzes nachrichtendienstlicher Mittel nach § 14 Abs. 1 Satz 1 Nrn. 7 bis 12 bedürfen der Zustimmung der G 10-Kommission (...)“.

¹⁷ Vgl. [Teil 4 B. II. 3. c.](#)

d. Funkzellenabfrage

Das rheinland-pfälzische Verfassungsschutzgesetz legt fest, dass Funkzellenabfragen genehmigungsbedürftig sind (§ 14 Abs. 2 S. 4 LVerfSchG RP i.V.m. § 2 Abs. 1 AG G10 RP).

e. Längerfristige Observationen

Obwohl alle 19 Nachrichtendienstgesetze Observationen ermöglichen, hat nur der niedersächsische Gesetzgeber festgelegt, dass längerfristige Observationen, „die innerhalb einer Woche insgesamt länger als 24 Stunden oder über einen Zeitraum von einer Woche hinaus durchgeführt“ werden, der Vorabkontrolle durch die G 10-Kommission unterliegen (§ 21 Abs. 3, 4 i.V.m. § 14 Abs. 2 Nr. 7 NVerfSchG). In Hessen, Bayern und Sachsen muss eine richterliche Genehmigung erteilt werden.¹⁸

f. Einsatz von Vertrauensleuten und Verdeckten Ermittlern

Bisher ordnen neben den richterlichen Genehmigungsvorbehalten im bayerischen, hessischen und sächsischen Verfassungsschutzgesetz¹⁹ nur zwei Nachrichtendienstgesetze beim Einsatz von Vertrauensleuten und Verdeckten Ermittlern eine unabhängige Vorabkontrolle an.

Wenn der niedersächsische Verfassungsschutz Verdeckte Ermittler einsetzen oder deren Einsatz verlängern möchte, muss die G 10-Kommission dies genehmigen (§ 21 Abs. 3, 4 i.V.m. § 14 Abs. 2 Nr. 9 NVerfSchG). Sie entscheidet auch, gegenüber welchen Beobachtungs- und Verdachtsobjekten Vertrauenspersonen eingesetzt werden und ob ihr Einsatz verlängert werden kann (§ 21 Abs. 5 S. 5 NVerfSchG, § 16 Abs. 3 S. 2 NVerfSchG). In Brandenburg wird die G 10-Kommission lediglich in einem sehr eng definierten Ausnahmefall eingebunden: Falls ein Verdeckter Ermittler oder eine Vertrauensperson weiter eingesetzt werden soll, obwohl bekannt geworden ist, dass er Straftaten begangen hat und eine interne Aufsichtsstelle des Verfassungsschutzes damit nicht einverstanden ist, muss diese die „Angelegenheiten“ der G 10-Kommission vorlegen (§ 6 a, b Abs. 2 BbgVerfSchG).²⁰

¹⁸ Vgl. [Teil 3 A. I. 1. b.](#)

¹⁹ Vgl. [Teil 3 A. I. 1. b.](#)

²⁰ Außerdem muss das PKGr unterrichtet werden. Für den Fall, dass Vertrauenspersonen oder Verdeckte Ermittler Straftaten begehen, sehen viele Verfassungsschutzgesetze eine Unterrichtung des PKGr vor.

g. Quellen-Telekommunikationsüberwachung

Der Bundesgesetzgeber hat die Befugnis zur Quellen-TKÜ in die Verfahrensvorschrift des § 11 G 10 integriert²¹ und bezeichnet sie als „technische Erweiterung“, die eine ursprüngliche Beschränkung ausfülle. Daher sei es ausreichend, wenn die G 10-Kommission über die ursprüngliche Beschränkung gem. § 15 Abs. 6 G 10 entscheide und vor ihrer „Erstreckung“ informiert werde.²² Über den Eingriff in das informationstechnische System wird die G 10-Kommission demnach nur unterrichtet, ihre Zustimmung ist jedoch nicht erforderlich. Ein Genehmigungsvorbehalt für die Quellen-TKÜ gem. § 11 Abs. 1a G 10 existiert deshalb nicht.

Vereinzelt waren Verfassungsschutzbehörden auf der Landesebene bereits zur Quellen-TKÜ berechtigt, bevor § 11 Abs. 1 G 10 verabschiedet wurde. Dort ist der Einsatz der Quellen-TKÜ von der Zustimmung der G 10-Kommission abhängig.²³

h. Online-Durchsuchung

Die Landesverfassungsschutzgesetze, die zur Online-Durchsuchung ermächtigen, ordnen an, dass die G 10-Kommission den Einsatz dieser Befugnis zu genehmigen hat²⁴ oder normieren einen Richtervorbehalt²⁵.

3. Genehmigungsvorbehalt zugunsten des Unabhängigen Kontrollrats des Bundes

Der UKRat ist für die Vorabkontrolle und die Datenschutzkontrolle der strategischen Ausland-Fernmeldeaufklärung und die damit einhergehenden Übermittlungen und Kooperationen des BND zuständig (§§ 40 Abs. 1, 42 Abs. 1 BNDG). Außerdem genehmigt er Eingriffe in informationstechnische Systeme von Ausländern im Ausland (§§ 42 Abs. 3, 4 BNDG).²⁶

²¹ Zu Recht kritisch insoweit *Poscher/Kappler*, Verfassungsblog vom 6.7.2021.

²² BR-Drs. 674/20, Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts v. 5.11.2020, S. 22, <https://dserver.bundestag.de/brd/2020/0674-20.pdf> (abgerufen am 31.8.2024).

²³ § 5d Abs. 3 *BWLVS*G, § 2 Abs. 2 *AG G 10 BW*; § 8 Abs. 12 *HmbVerfSchG*, § 15 G 10.

²⁴ § 5d Abs. 3 *BWLVS*G, § 2 Abs. 2 *AG G 10 BW*; § 8 Abs. 12 *HmbVerfSchG*, § 15 G 10.

²⁵ Art. 11 Abs. 1, Art. 10 *BayVSG*. Zudem soll grundsätzlich über die Verwertbarkeit der erhobenen personenbezogenen Daten eine richterliche Entscheidung herbeigeführt werden, vgl. Art. 11 Abs. 2 S. 3, Abs. 4 *BayVSG*.

²⁶ *Graulich*, GSZ 2021, 121, 128.

II. Änderungsbedarf

Wo Vorabkontrollen durch die G 10-Kommissionen normiert wurden, müssen die Normen um die Festlegung ergänzt werden, dass die Genehmigung bei länger andauernden Maßnahmen erneuert werden muss. Die niedersächsische G 10-Kommission entscheidet gem. § 21 Abs. 3 NVerfSchG bereits nach geltendem Recht über Verlängerungen der Maßnahmen.

Im Ergebnis müssen jedoch für eine Vielzahl nachrichtendienstlicher Befugnisse von (besonders) schwerer Eingriffsintensität bundesweit überhaupt erst unabhängige Vorabkontrollen eingeführt werden.

1. Langfristige Observationen

Dies betrifft zunächst die langfristigen Observationen. Nur in Niedersachsen, Bayern, Hessen und Sachsen sind unabhängige Vorabkontrollen normiert.²⁷

Alle anderen Fachgesetze sind insoweit verfassungswidrig.²⁸

2. Einsatz von Vertrauensleuten und Verdeckten Ermittlern

Unabhängige richterliche oder richterähnliche Vorabkontrollen des Einsatzes von Verdeckten Ermittlern oder Vertrauenspersonen sind de lege lata nur in Niedersachsen, Bayern, Hessen und Sachsen vorgesehen.²⁹

Alle anderen Nachrichtendienstgesetze sind insoweit verfassungswidrig. Auch ein Zustimmungsvorbehalt zugunsten des Parlamentarischen Kontrollgremiums wie beispielsweise in § 8b Abs. 5 BremVerfSchG ändert daran nichts, da die Kontrolle des PKGr nicht richterähnlich konzipiert ist.

Wenn Erhebungen aus öffentlich zugänglichen Social Media in einer Weise erfolgen, dass man von einem Einsatz von Vertrauensleuten oder Verdeckten Mitarbeitern „mit anderen Mitteln“ sprechen kann³⁰, muss auch dafür ein Richtervorbehalt vorgesehen werden.

²⁷ Die Regelungen in Bayern und Sachsen sehen die Vorabkontrollen allerdings erst ab einem zu späten Zeitpunkt vor, sodass auch diese Regelungen verfassungswidrig sind, vgl. zur bayrischen Regelung S. 404.

²⁸ In den Fachgesetzen, die de lege lata nicht zwischen nicht-langfristigen und langfristigen Observationen differenzieren, muss eine Vorabkontrolle für die Observations-Ermächtigung ergänzt werden.

²⁹ Vgl. [Teil 3 A. I. 2. f.](#); wobei die Regelungen in Bayern und Sachsen den Genehmigungsvorbehalt erst zu einem so späten Zeitpunkt anordnen, dass auch sie den Vorgaben des Bundesverfassungsgerichts nicht entsprechen, vgl. zur bayerischen Regelung [Teil 4 B. II. 3. b.](#)

³⁰ Vgl. [Teil 2 A. III. 4. b. cc\) \(1\).](#)

3. IMSI/IMEI-Catcher

In den Verfassungsschutzgesetzen von Brandenburg, Thüringen und dem Saarland muss der Einsatz technischer Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes oder zur Ermittlung der Geräte- oder Kartennummer noch mit dem Vorbehalt der Genehmigung durch eine unabhängige Stelle verbunden werden, um verfassungskonform zu sein.³¹

B. Rechtskontrolle der G 10-Kommissionen

Die G 10-Kommissionen sind de lege lata für die externe Kontrolle der Nachrichtendienste von enormer Bedeutung. Obwohl die Rechtsgrundlagen der G 10-Kontrolle auf der Landesebene am Bundesrecht orientiert und teilweise übereinstimmend formuliert sind, zeigen sich im Detail sehr weitreichende Unterschiede.

Ohne die überwiegende³² Auskunftsbereitschaft der Verantwortlichen in den Bundesländern gegenüber Anfragen der Autorin wäre diese vergleichende Darstellung nicht realisierbar gewesen, weil die gesetzlichen Grundlagen ohne Einblicke in die nicht-öffentlichen Geschäftsordnungen und ohne Informationen über die parlamentarische Praxis nur bedingt aussagekräftig sind. Dennoch muss betont werden, dass leider nicht jede Geschäftsordnung gelesen werden durfte, was bedeutet, dass die Darstellung der Rechtslage in diesen Ländern mit an Sicherheit grenzender Wahrscheinlichkeit nicht vollständig ist.³³

Positiv ist hervorzuheben, dass die Geschäftsordnung der G 10-Kommission des Bundes vom 7. Juli 2022 auf der Website des Bundestags öffentlich zugänglich ist.³⁴

³¹ Alternativ könnte das bayerische Regelungsmodell gewählt werden, wonach der Einsatz der technischen Mittel begrenzt und die Eingriffsintensität gemindert wird, um die Notwendigkeit einer Vorabkontrolle zu vermeiden.

³² Die Landtagsverwaltungen bzw. G 10-Kommissionen von Hamburg, Sachsen-Anhalt und Niedersachsen haben bedauerlicherweise nicht geantwortet.

³³ Dies betrifft Nordrhein-Westfalen, Niedersachsen, Rheinland-Pfalz, Berlin, Brandenburg, Bayern, Sachsen-Anhalt, Mecklenburg-Vorpommern, das Saarland, Hessen (die hessische G 10-Kommission begründet die Weigerung damit, dass die Geschäftsordnung selbst „Ausfluss der Beratungen“ sei und deshalb ebenfalls der Geheimhaltung unterläge, E-Mail v. 29.3.2023), Hamburg, wo mit der Beantwortung eine Kanzlei beauftragt wurde, die inhaltlich nie geantwortet hat.

³⁴ https://www.bundestag.de/ausschuesse/weitere_gremien/g10_kommission/geschaeftsordnung-932190 (abgerufen am 31.8.2024).

I. Kontrollmaßstab

Alle achtzehn G 10-Kommissionen sollen die Rechtmäßigkeit³⁵ bestimmter Entscheidungen überprüfen, ihr Kontrollmaßstab ist identisch.

II. Kontrollgegenstand und -tiefe

Die G 10-Kommissionen genehmigen den Einsatz von bestimmten nachrichtendienstlichen Mitteln (1.), entscheiden über die Benachrichtigung Betroffener (2.) und prüfen die Rechtmäßigkeit der Datenverarbeitungen (3.).

1. Vorabkontrolle

Hinsichtlich der Vorabkontrolle ist der Normal- vom Eilfall zu unterscheiden.

a. Grundsatz

Erstens entscheidet die G 10-Kommission „über die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen“ vor deren Vollzug.³⁶

Eine Beschränkung ist gem. § 15 Abs. 5 S. 1, Abs. 6 G 10 zulässig, wenn sie rechtmäßig ist.³⁷ Notwendig ist eine Maßnahme, die verhältnismäßig und insbesondere erforderlich ist. Das bedeutet, es darf kein milderes Mittel zur Sachverhaltsaufklärung ersichtlich sein.³⁸

Die G 10-Kommission ist zunächst zuständig für die Rechtskontrolle von Maßnahmen nach dem G 10: Sie genehmigt Telekommunikationsüberwachungen (§ 3 G 10) und einen Teil³⁹ der strategischen Überwachungen durch den BND (§ 5 G 10). In den Anträgen für Maßnahmen zur strategischen Überwachung gem. § 5 G 10 werden die benutzten Suchbegriffe erläutert, sodass sich die Genehmigung der G 10-Kommission darauf erstreckt.⁴⁰

³⁵ Bantlin, G 10-Kommission, S. 157.

³⁶ Diese Formulierung ist in allen G 10 identisch: § 15 Abs. 5 S. 1, Abs. 6 G 10; § 30 Abs. 5 S. 1 VSG NRW; § 2 Abs. 2 S. 2 AG G 10 BW; § 4 Abs. 1 S. 1 HAGG 10; § 2 Abs. 1 S. 1 AG G 10 RP; § 3 Abs. 6 S. 1 G10DGS; § 4 Abs. 1 S. 1 Nds. AG G 10; § 1 Abs. 3 S. 1 HmbG10AusfG; § 3 Abs. 1 S. 3 AG G10 Bremen; § 26a Abs. 1 S. 2 LVerfSchG SH; § 15 Abs. 5 G 10; § 2 Abs. 1 S. 3 AG G 10 MV; § 3 Abs. 1 S. 3 G10AG-Bbg; § 2 Abs. 1 S. 3 AG G 10 Bln; § 2 Abs. 1 S. 4 Sächs AGG 10; § 3 Abs. 1 S. 4 AG G 10 TH; § 5 Abs. 1 S. 1 AG G 10-LSA; Art. 2 Abs. 1 S. 3 AGG 10BY.

³⁷ Bantlin, G 10-Kommission, S. 122; nach Huber ist dafür lediglich eine Rechtsgrundlage notwendig, Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 42.

³⁸ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 42; Bantlin, G 10-Kommission, S. 122.

³⁹ Die strategische Ausland-Fernmeldeaufklärung gem. §§ 19 ff. BNDG genehmigt hingegen das Ge-Kon, vgl. Teil 3 C II. 1.

⁴⁰ Huber, NVwZ-Beilage 2021, 3, 5; Roggan, § 15 G 10 Rn. 14.

Darüber hinaus ist sie auf der Bundesebene zuständig für die Genehmigung besonderer Auskunftsverlangen (§ 8b Abs. 2 BVerfSchG) und des Einsatzes von IMSI/IMEI-Catchern (§§ 9 Abs. 4 BVerfSchG i.V.m. 8b Abs. 2 BVerfSchG).

Auch in einigen Ländern sind die G 10-Kommissionen neben der Genehmigung von Telekommunikationsüberwachungen für die Vorabkontrolle anderer nachrichtendienstlicher Maßnahmen zuständig.⁴¹

Darüber hinaus wurden ihr vereinzelt weitere Aufgaben übertragen. So muss die niedersächsische G 10-Kommission teilweise zustimmen, wenn bei der Übermittlung an Staatsanwaltschaften und Polizeibehörden des Landes auf die Kennzeichnung personenbezogener Daten verzichtet werden soll (§ 31 Abs. 2 S. 2 NVerfSchG, § 8 Abs. 9 S. 2 LVerfSchG SH).

b. Ausnahme: Eilfall

Von diesem grundsätzlichen Genehmigungsvorbehalt können bei Gefahr im Verzug Ausnahmen gemacht werden, indem Beschränkungen auch ohne eine vorherige Entscheidung der G 10-Kommission vollzogen werden (Eilanordnung).⁴² Eine solche Eilanordnung muss auf der Bundesebene jedoch innerhalb von drei „Werktagen“ durch den Vorsitzenden oder einen Stellvertreter bestätigt und die Prüfung der Zulässigkeit und Notwendigkeit dieser Maßnahme durch die Kommission „unverzüglich“ nachgeholt werden (§ 15a Abs. 2 S. 1 G 10). Gem. § 3 Abs. 7 S. 2 G10DGS ist die Unterrichtung der G 10-Kommission innerhalb von maximal zwei Tagen nachzuholen. Teilweise ist die Unterrichtung der Kommission „unverzüglich“ nachzuholen.⁴³ Wie der Begriff „unverzüglich“ zu verstehen ist, wird nicht erörtert.⁴⁴ Würde man die Legaldefinition aus § 121 Abs. 1 BGB („ohne schuldhaftes Zögern“) übertragen⁴⁵, wäre dennoch nichts darüber gesagt, ob die Kommission oder einer ihrer Vertreter entsprechend den Vorga-

⁴¹ Vgl. [Teil 3 A. I. 2.](#)

⁴² § 15a Abs. 1 S. 4 [G 10](#); § 5b Abs. 1 S. 4 [VSG NRW](#); § 2 Abs. 2 S. 3 [AG G 10 BW](#); § 3 Abs. 2 [HAGG10](#); § 3 Abs. 2 [AG G 10 RP](#); § 3 Abs. 7 S. 2 [G10DGS](#); § 4 Abs. 1 S. 3 [Nds. AG G 10](#); § 1 Abs. 2 S. 2 [HmbG10AusfG](#); § 3 Abs. 1 S. 2 [AG G10 Bremen](#); § 8b Abs. 2 S. 2 [LVerfSchG SH](#); § 2 Abs. 1 S. 2 [AG G 10 MV](#); § 3 Abs. 1 S. 2 [G10AGBbg](#); § 2 Abs. 1 S. 2 [AG G10 Bln](#); § 2 Abs. 1 S. 2 [Sächs AGG10](#); § 3 Abs. 1 S. 2 [AG G 10 TH](#); § 5 Abs. 1 S. 3 [AG G 10-LSA](#); Art. 2 Abs. 1 S. 2 [AGG10BY](#).

⁴³ Baden-Württemberg, Hessen, Rheinland-Pfalz, Niedersachsen.

⁴⁴ In der Gesetzesbegründung zu § 15a G 10 heißt es, das vorläufig entscheidende Mitglied könne dazu eine Sondersitzung der Kommission initiieren, wenn die Umstände des Einzelfalls dies veranlassten, BT-Drs. 674/20, Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts v. 5.11.2020, S. 24. Demnach wird „unverzüglich“ offenbar weiter verstanden als die drei Werktage, innerhalb derer ein Mitglied vorläufig zu entscheiden hat.

⁴⁵ Der Hinweis auf § 121 Abs. 1 BGB ist von Mitarbeitern zweier G 10-Kommissionen erteilt worden. In der Regel sei dies „der erste Werktag, der auf den Tag folgt, an dem der fachlich zuständige Minister den Vollzug (...) angeordnet hat“, heißt es in der Antwort aus dem rheinland-pfälzischen Landtag.

ben aus der Rechtsprechung des EGMR innerhalb von 72 Stunden zwingend zu benachrichtigen sind. Soweit der Begriff so ausgelegt wird, dass die Vorabkontrolle spätestens drei Tage nach der Eilanordnung erfolgt, bestehen keine Bedenken zur Konventionskonformität.⁴⁶

Anders ist dies zu beurteilen, wenn wie in acht Bundesländern ein Zuwarten von bis zu maximal zwei Wochen ermöglicht wird, bevor die G 10-Kommission zu benachrichtigen ist⁴⁷ oder wenn die Norm zur Eilanordnung wie in Bremen und Schleswig-Holstein keine nachträgliche Genehmigung vorsieht⁴⁸. Diese Normen sind konventionswidrig.⁴⁹

Während einige Fachgesetze explizit so formuliert sind, dass die G 10-Kommission nachträglich eine Entscheidung trifft⁵⁰, ist in den meisten Gesetzen lediglich eine Unterrichtung⁵¹ vorgesehen. Falls die Kommission nur informiert wird und der Maßnahme nicht nachträglich zustimmen muss, sind diese Normen verfassungs- und konventionswidrig. Es ist jedoch wahrscheinlicher, dass es sich dabei um eine sprachliche Unschärfe handelt und die G 10-Kommissionen nachträglich zustimmen müssen. Hier besteht Klärungsbedarf.

2. Entscheidung über die Benachrichtigung Betroffener

Zweitens ist die G 10-Kommission in die Benachrichtigung der Betroffenen eingebunden: Sie wird darüber benachrichtigt, ob die Mitteilung an Betroffene erfolgt ist bzw. welche Gründe gegen eine Benachrichtigung sprechen (§ 15 Abs. 7 G 10). Wenn die

⁴⁶ Vgl. [Teil 2 B. I. 4. a. aa](#)), *Huber*, GSZ 2017, 12, 16. Streng genommen müsste § 15a G 10 Abs. 2 S. 1 von „Tagen“ statt „Werktagen“ sprechen, um diese Vorgabe zu erfüllen.

⁴⁷ § 1 Abs. 2 S. 2 [HmbG10AusfG](#); § 2 Abs. 1 S. 2 [AG G 10 MV](#); § 3 Abs. 1 S. 2 [G10AGBbg](#); § 2 Abs. 1 S. 2 [AG G10 Bln](#); § 2 Abs. 1 S. 2 [Sächs AGG10](#); § 3 Abs. 1 S. 3 [AG G 10 TH](#); § 5 Abs. 1 S. 4 [AG G 10-LSA](#); Art. 2 Abs. 1 S. 2 [AGG10BY](#).

⁴⁸ Vgl. § 3 Abs. 1 [AG G10 Bremen](#); § 8b Abs. 2 [LVerfSchG SH](#). Die zur Verfügung gestellte Geschäftsordnung der G 10-Kommission Bremen verpflichtet die Kommission ebenfalls nicht zur nachträglichen Genehmigung.

⁴⁹ Ebenso zur mittlerweile überholten Rechtslage auf Bundesebene, *Huber*, GSZ 2017, 12, 16.

⁵⁰ § 15a Abs. 2 S. 1 G 10; § 5b Abs. 1 S. 4 [VSG NRW](#); § 4 Abs. 1 S. 4 [Nds. AG G 10](#); § 5 Abs. 1 S. 4 [AGG10LSA](#).

⁵¹ § 2 Abs. 2 S. 4 [AG G 10 BW](#); § 3 Abs. 2 [AG G 10 RP](#); § 2 Abs. 2 S. 2 [HAGG10](#); § 3 Abs. 7 S. 2 [G10DGSL](#); § 1 Abs. 2 S. 2 [HmbG10AusfG](#); § 2 Abs. 1 S. 2 [AG G 10 MV](#); § 3 Abs. 1 S. 2 [G10AGBbg](#); § 2 Abs. 1 S. 2 [AG G10 Bln](#); § 2 Abs. 1 S. 2 [Sächs AGG10](#); § 3 Abs. 1 S. 3 [AG G 10 TH](#); Art. 2 Abs. 1 S. 2 [AGG10BY](#).

Kommission entscheidet, dass eine Mitteilung geboten ist, muss der Nachrichtendienst die Mitteilung nachholen.⁵²

3. Datenschutzkontrolle

Drittens kontrolliert die G 10-Kommission die „gesamte Verarbeitung“ der nach dem G 10 erlangten personenbezogenen Daten einschließlich ihrer Übermittlung an andere Behörden.⁵³

Darüber ist die G 10-Kommission in den meisten Gesetzen auch für die laufende und nachträgliche Kontrolle der weiteren Datenverarbeitungen, die sie genehmigt, zuständig.⁵⁴

Für die Datenschutzkontrollen dieser Verarbeitungen sind die G 10-Kommissionen überwiegend ausschließlich zuständig, die Zuständigkeit der Datenschutzbeauftragten wird insoweit begrenzt.⁵⁵ Vereinzelt gilt die Zuständigkeitsbegrenzung des Datenschutzbeauftragten jedoch nur für die Verarbeitung von Daten nach dem G 10, erstreckt sich also nicht auf nachrichtendienstliche Befugnisse außerhalb des G 10, die die G 10-Kommission genehmigt.⁵⁶ In vier der Landesgesetze, die nicht nur weitere Genehmigungsvorbehalte, sondern auch die anschließende Datenschutzkontrolle dieser Daten der G 10-Kommission übertragen, gibt es keine Norm, die insoweit eine alleinige

⁵² § 15 Abs. 7 G 10; § 4 Abs. 5, 6 [Nds. AG G 10](#); § 26a Abs. 1 S. 2 [LVerfSchG SH](#), § 15 Abs. 7 G 10; „einschließlich der Entscheidung über die Mitteilung an Betroffene“ sei die G 10-Kommission für die Kontrolle zuständig, § 30 Abs. 5 S. 2 [VSG NRW](#); § 2 Abs. 3, 4 S. 1 [AG G 10 BW](#); § 4 Abs. 1 S. 2 [HAGG10](#); § 2 Abs. 3 [AG G 10 RP](#); § 3 Abs. 6 [G10DGSL](#); § 1 Abs. 5 [HmbG10AusfG](#); § 3 Abs. 1 S. 4 [AG G10 Bremen](#); § 2 Abs. 1 S. 4 [AG G 10 MV](#); § 3 Abs. 2 [G10AGBbg](#); § 2 Abs. 2 [AG G10 Bln](#); § 2 Abs. 3 [Sächs AGG10](#); § 4 [AG G 10 TH](#); § 6 Abs. 1 [AG G 10-LSA](#); Art. 2 Abs. 4 [AGG10BY](#). Dazu im Detail *Bartodziej*, Hdb. des Rechts der Nachrichtendienste, 1533, 1592 f.

⁵³ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 46; § 15 Abs. 5 S. 2 G 10; § 30 Abs. 5 S. 2 [VSG NRW](#); § 2 Abs. 4 S. 1 [AG G 10 BW](#); § 4 Abs. 1 S. 2 [HAGG10](#); § 2 Abs. 3 S. 1 [AG G 10 RP](#); § 3 Abs. 6 S. 2 [G10DGSL](#); § 4 Abs. 2 S. 1 [Nds. AG G 10](#); § 1 Abs. 5 S. 1 [HmbG10AusfG](#); § 3 Abs. 1 S. 4 [AG G10 Bremen](#); § 26a Abs. 1 [LVerfSchG SH](#), § 15 Abs. 5 G 10; § 2 Abs. 1 S. 4 [AG G 10 MV](#); § 3 Abs. 1 S. 5 [G10AGBbg](#); § 2 Abs. 2 S. 1 [AG G 10 Bln](#); § 2 Abs. 2 S. 1 [Sächs AGG10](#); § 3 Abs. 2 S. 1 [AG G 10 TH](#); § 5 Abs. 2 S. 1 [AG G 10-LSA](#); Art. 2 Abs. 2 [AGG10BY](#).

⁵⁴ § 15 Abs. 5 G 10, § 8b Abs. 2 S. 4 BVerfSchG; § 5b Abs. 6 S. 3 [BWLVSg](#); § 10 Abs. 5 S. 7 [HVSG](#), § 15 Abs. 5 G 10; § 13 Abs. 7 [LVerfSchG RP](#), § 2 Abs. 3 [AG G 10 RP](#); § 7a Abs. 2, § 1 Abs. 5 S. 1 [HmbG10AusfG](#); § 8b Abs. 2 S. 4 [LVerfSchG SH](#); § 24a Abs. 4 S. 4 [VerfSchG MV](#); § 14a Abs. 5 S. 6 [Bbg-VerfSchG](#), § 15 Abs. 5 G 10; § 27a Abs. 5 S. 7 [VSG Bln](#); § 16 Abs. 2 [SächsVSG](#); § 2 Abs. 2 [SächsAG G10](#); § 8 Abs. 4 S. 5 [ThürVerfSchG](#); § 17a Abs. 5 S. 4 [VerfSchG LSA](#).

⁵⁵ § 28 Abs. 2 S. 2 BVerfSchG (§ 63 [BNDG](#) bzw. § 13 a [MADG](#), § 28 Abs. 2 S. 2 BVerfSchG); § 17 Abs. 1 S. 2 [BWLVSg](#); § 30 Abs. 1 S. 2 [LVerfSchG RP](#); § 15 Abs. 2 S. 3 [VSG NRW](#); § 23b Abs. 2 S. 2 [Hmb-VerfSchG](#); § 39 Abs. 1 S. 1 [SächsVSG](#); Umkehrschluss aus § 5 Abs. 3 S. 1 [AG G 10-LSA](#); § 32a Abs. 2 S. 2 [VSG Bln](#); *Aden*, Vorgänge 2015, 245, 248.

⁵⁶ § 3 Abs. 1 [AG G 10 MV](#) wegen der Beschränkung auf Datenverarbeitungen nach dem AG G 10.

Zuständigkeit der G 10-Kommission begründet.⁵⁷ Dort ist neben der G 10-Kommission auch der Landesdatenschutzbeauftragte für die Datenschutzkontrolle von Datenverarbeitungen, deren Erhebung die G 10-Kommission genehmigt hat, zuständig.

Eine weitere Aufgabe der Kommission besteht darin, Beschränkungsmaßnahmen zu prüfen, weil Betroffene sich mit einer Eingabe an sie gewandt haben. Sie wird bereits tätig, wenn „jemand auch nur den vagen Verdacht äußert, dass von einem Nachrichtendienst in das Grundrecht aus Art. 10 Abs. 1 GG eingegriffen worden ist“.⁵⁸

III. Zeitpunkt

Der Zeitpunkt der Kontrolle durch die G 10-Kommission ist abhängig von der Aufgabe, die sie wahrnimmt. Während die Vorabkontrolle im Regelfall ex-ante stattfindet, kann die Datenschutzkontrolle jederzeit und unabhängig von konkreten Beschränkungsmaßnahmen erfolgen⁵⁹.

IV. Kontrolleur

Wie die G 10-Kommission konzipiert ist, ergibt sich aus dem Zusammenspiel unterschiedlicher Faktoren: Es kommt darauf an, wie viele Mitglieder sie hat (1.) und auf welche Weise diese ernannt werden (2.), wer diese Tätigkeit ausübt (3.), wie die Entscheidungen getroffen werden (4.) und welche Vorkehrungen zur Geheimhaltung getroffen werden (5.).

1. Anzahl der (stellvertretenden) Mitglieder

Auf der Bundesebene und in fast allen Bundesländern setzt sich die Kommission aus einer bestimmten Anzahl ordentlicher Mitglieder und einer entsprechenden Anzahl stellvertretender Mitglieder zusammen. Die G 10-Kommission des Bundes und die G 10-Kommission in Nordrhein-Westfalen und Hamburg sind die größten Gremien, sie haben jeweils fünf ordentliche Mitglieder und fünf stellvertretende Mitglieder.⁶⁰ In

⁵⁷ In Hessen, Schleswig-Holstein, Brandenburg und Thüringen gibt es keine dem § 28 Abs. 2 BVerfSchG vergleichbare Norm.

⁵⁸ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 36 f., wobei die Anzahl der Beschwerden gering ist, Bartodziej, Hdb. des Rechts der Nachrichtendienste, 1533, 1593 Rn. 112. Soweit eine Beschränkung angeordnet bzw. vollzogen wurde, kann die G 10-Kommission in einen Interessenskonflikt geraten, wenn eine Mitteilung an den Betroffenen (zu diesem Zeitpunkt) nicht erfolgen darf, dazu Roggan, § 15 G 10 Rn. 12; Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 40.

⁵⁹ Bartodziej, Hdb. des Rechts der Nachrichtendienste, 1533, 1593.

⁶⁰ § 15 Abs. 1 S. 1 G 10; § 30 Abs. 1 S. 2 VSG NRW; § 2 Abs. 1 S. 1 HmbG10AusfG, bei Hamburg verwundert dies insoweit, als die Verfassungsschutzbehörde nicht zu den bundesweit zahlenmäßig größten gehört.

zwei Ländern sind vier ordentliche und vier stellvertretende Mitglieder vorgesehen.⁶¹ Acht Landesgesetze legen fest, dass die Kommission aus drei ordentlichen und drei stellvertretenden Mitgliedern besteht.⁶² Vereinzelt sollen ausschließlich ordentliche Mitglieder, aber keine Stellvertreter berufen werden.⁶³ Teilweise wird die Anzahl der Mitglieder offengelassen⁶⁴ oder an die Anzahl der im Landtag vertretenen Fraktionen geknüpft⁶⁵.

Wenn Stellvertreter benannt werden, hat dies den Vorteil, dass die Kommission stets entscheidungsfähig ist. Gem. § 15 Abs. 1 S. 1 G 10 (i.V.m. § 3 Abs. 3 GO G 10) dürfen die Vertreter an den Sitzungen teilnehmen, sich zu Wort melden und Fragen stellen. Jedenfalls auf der Bundesebene machen die Vertreter davon auch Gebrauch, um im Vertretungsfall eingearbeitet zu sein.⁶⁶ In drei Ländern wurde eine ähnliche Formulierung übernommen, sodass den Stellvertretern dort ebenfalls Teilnahme-, Rede- und Fragerechte verliehen wurden.⁶⁷ In vier Ländern nehmen die Stellvertreter nur dann teil, wenn ein Mitglied der Kommission verhindert ist.⁶⁸

In den übrigen Ländern könnten solche Rechte in den Geschäftsordnungen der G 10-Kommissionen etabliert sein.⁶⁹ Wo diese (leider) nicht zur Verfügung gestellt werden und teilweise sogar explizit als Verschlussache eingestuft sind, ist dies jedoch nicht prüfbar.⁷⁰

⁶¹ § 2 Abs. 3 S. 1, Abs. 5 [AG G 10 MV](#); § 4 Abs. 1 S. 2, 3 [AG G 10 LSA](#).

⁶² § 2 Abs. 5 S. 1, 4 [AG G 10 BW](#); § 5 Abs. 1 S. 1, 5 [HAGG10](#); § 3 Abs. 1 S. 1, 4 [Nds. AG G 10](#); § 3 Abs. 3 S. 1, 4 [AG G 10 Bremen](#); § 26a Abs. 2 S. 1, 3 [LVerfSchG SH](#); § 2 Abs. 1 S. 3, 4 [G10AGBbg](#); § 3 Abs. 1 S. 1, 4 [Sächs AGG10](#); Art. 2 Abs. 6 S. 1, 4 [AGG10BY](#).

⁶³ § 1 Abs. 2 S. 1 [AG G 10 RP](#); § 2 Abs. 2 S. 1 [AG G 10 TH](#), wobei die Kommission nach Mitteilung des Geschäftsführers 2023 nur aus zwei Mitgliedern besteht, nach Auskunft des Geschäftsführers der Kommission auch im Saarland.

⁶⁴ § 3 Abs. 1 [G10DGSL](#), wo die Mitgliederanzahl der des Parlamentarischen Kontrollgremiums entspricht, dessen Anzahl aber im Gesetz nicht geregelt ist. Aktuell besteht es aus zwei Mitgliedern (2023).

⁶⁵ § 2 Abs. 4 [AG G 10 Bln](#).

⁶⁶ So schildert es Bertold Huber, der amtierende Vorsitzende der Kommission in Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 19.

⁶⁷ § 3 Abs. 1 S. 5 [Nds. AG G 10](#); § 26a Abs. 2 S. 3 [LVerfSchG SH](#); Teilnahmerecht gem. § 3 Abs. 2 GO G 10 Bremen.

⁶⁸ Baden-Württemberg, Sachsen, Hessen und Bayern.

⁶⁹ Aus dem Umkehrschluss aus § 3 Abs. 2 GO Bremen, nach der Stellvertreter kein Stimmrecht haben, wenn der Vertretungsfall nicht eingetreten ist, ergibt sich, dass ihnen ein Teilnahme-, Rede- und Fragerecht zukommt.

⁷⁰ Wieso nicht nur die Arbeitsweise des Kontrollierten, sondern auch die des Kontrolleurs geheim sein muss, erschließt sich nicht. Bei den Verantwortlichen in Bremen, Baden-Württemberg, Brandenburg, Sachsen, Thüringen und Schleswig-Holstein, die offenbar keine Geheimhaltungsbedenken umtreiben und die ihre GO für diese Ausarbeitung zur Verfügung gestellt haben, bedanke ich mich herzlich.

2. Ernennung der G 10-Kommission

Die Mitglieder der G 10-Kommissionen werden zwar nur für eine Wahlperiode ernannt, sie bleiben jedoch so lange im Amt, bis eine neue Kommission ernannt wurde⁷¹ oder bis maximal drei Monate nach dem Ende der Wahlperiode⁷².

a. Wahl der Mitglieder

Die G 10-Kommission wird entweder durch das Plenum des Parlaments⁷³ oder das jeweilige PKGr gewählt.⁷⁴ Vereinzelt darf jede Fraktion des Landtags ein Mitglied und einen Vertreter vorschlagen.⁷⁵ Teilweise wird die Regierung vor der Wahl angehört.⁷⁶ Um die Unabhängigkeit der Kommissionen abzusichern, ist eine Abwahl nicht vorgesehen.⁷⁷

b. Anbindung an die Legislative

Dass die G 10-Kommission vom Parlament gewählt wird, ergibt sich seit der Verfassungsänderung von 1968 direkt aus Art. 10 Abs. 2 S. 2 GG, wonach „an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt“. Diese Anbindung an die Legislative wird jedoch kritisiert: Die Kontrolle sei einer unabhängigen gerichtlichen Kontrolle nicht gleichwertig, weil die Mitgliederwahl durch das „Stärkeverhältnis der Fraktionen“ bestimmt sei und die G 10-Kommission daher „von der jeweiligen parlamentarischen Regierungsmehrheit dominiert“ werde, auch die „Weisungsfreiheit“ könne dies nicht kompensieren.“⁷⁸ Steinke verdeutlicht die Dominanz der regierungstragenden Fraktionen bei der Auswahl der Mitglieder:

„Nichts überlassen die Parteien, die jeweils die Regierung stellen, hier dem Zufall. Seit 2021 besetzen die drei Ampelparteien SPD, Grüne

⁷¹ § 15 Abs. 1 S. 4 G 10; § 30 Abs. 1 S. 4 [VSG NRW](#); § 2 Abs. 5 S. 5 [AG G 10 BW](#); § 5 Abs. 1 S. 6 [HAGG 10](#); § 3 Abs. 1 S. 3 [Nds. AG G 10](#); § 2 Abs. 1 S. 5 [HmbG10AusfG](#); § 3 Abs. 3 S. 5 [AG G10 Bremen](#); § 3 Abs. 1 S. 5 [Sächs AGG 10](#); § 4 Abs. 1 S. 4 [AG G 10-LSA](#); Art. 2 Abs. 6 S. 5 [AGG 10BY](#).

⁷² § 1 Abs. 2 S. 2 [AG G 10 RP](#); § 3 Abs. 2 S. 2, 3 [G10DGS L](#); § 26a Abs. 2 S. 2 [LVerfSchG SH](#); § 2 Abs. 3 S. 3 [AG G 10 MV](#); § 2 Abs. 2 S. 2 [G10AGBbg](#); § 2 Abs. 4 S. 3 [AG G10 Bln](#); § 2 Abs. 2 S. 2 [AGG 10 TH](#).

⁷³ Baden-Württemberg; Rheinland-Pfalz; Hamburg; Schleswig-Holstein; Mecklenburg-Vorpommern; Brandenburg; Berlin; Sachsen; Thüringen; Bayern.

⁷⁴ Bund, Nordrhein-Westfalen, Saarland, Niedersachsen, Bremen, Sachsen-Anhalt.

⁷⁵ Brandenburg, Berlin.

⁷⁶ Bund, Nordrhein-Westfalen, Saarland, Niedersachsen.

⁷⁷ Zu G 10-Kommission des Bundes Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 23, auch die anderen Gesetze ermöglichen keine Abwahl.

⁷⁸ *Deiseroth*, ZRP 2013, 196; *Steinke*, Verfassungsschutz, S. 63 f.

*und FDP zum Beispiel sieben der zehn Posten. So haben sie es zu Beginn der Legislaturperiode untereinander ausgehandelt. Nur die verbleibenden drei Sitze, eine kleine Minderheit, gingen an die Union als einzige Oppositionspartei. Die Linkspartei und die AfD hat man ganz hinausgedrängt.*⁷⁹

Dem ist entgegenzuhalten, dass die Ernennung von Richtern auf der Bundesbene und in einigen Bundesländern ebenfalls politisch ist, weil die Richter von Richterwahlausschüssen benannt werden, denen Minister oder Landtagsabgeordnete angehören.⁸⁰ Wenn man die Kontrolle durch alternative Kontrolleure wegen der Besonderheiten des Nachrichtendienstrechts als grundsätzlich legitim anerkennt, ist die Wahl durch das Parlament die vorzuzugswürdige Option. Die Ernennung der Kontrolleure durch die Exekutive, deren Handeln gerade Kontrollgegenstand ist, kommt demgegenüber nicht in Betracht. Für die Wahl durch die Legislative spricht zudem, dass die Kontrolleure auf diese Weise demokratisch legitimiert werden.⁸¹

Der EGMR hat unter anderem eine Benennung durch die Legislative als wünschenswert eingestuft, hier aber vorausgesetzt, dass auch Vertreter der Opposition Berücksichtigung finden.⁸² Ob mindestens ein Vorschlag der Opposition erfolgreich sein muss, ergibt sich aus den Gesetzen jedoch nicht.

Um die Berücksichtigung der Opposition sicherzustellen, könnte eine so hohe qualifizierte Mehrheit für die Wahl der Mitglieder vorgeschrieben werden, dass eine Mehrheit ohne die Stimmen einzelner Oppositionsfraktionen nicht zustande kommen kann. Andererseits würde das den Wahlprozess verkomplizieren. Dabei wäre es wichtig, das Quorum nicht so hoch anzusetzen, dass Blockaden der Opposition die Funktionsfähigkeit der G 10-Kommission beeinträchtigen könnten.

⁷⁹ *Steinke*, Verfassungsschutz, S. 63.

⁸⁰ Vgl. z.B. § 1 Abs. 1, §§ 2 ff. RiWG; § 15, 14 Abs. 1 LRiG RP.

⁸¹ "If the problem for parliamentary accountability bodies can be summarized in the word 'competence', the problem for expert bodies can be summarized in the word 'legitimacy' (...) Moreover, in order to maintain parliament's confidence in the expert body it is necessary to provide for institutional links between the two.", *Venedig-Kommission*, Report 2015, S. 51 Rn. 231; *Roggan*, § 15 G 10 Rn. 4.

⁸² Vgl. [Teil 3 B. II. 1.](#); EGMR 4.12.2015 – 47143/06 Rn. 278 – Roman Zakharov gg. Russland: "As to the independence requirement, in previous cases the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it found sufficiently independent bodies composed of members of parliament of both the majority and the opposition (...)". Andererseits hat der EGMR in einer Entscheidung zur deutschen Kontrollarchitektur 1978 die G 10-Kommission und die Parlamentarische Kontrollkommission (Vorgänger des PKGr) gemeinsam betrachtet und insoweit festgestellt, dass eine ausreichende Unabhängigkeit deshalb anzunehmen wäre, weil in der Parlamentarische Kontrollkommission auch die Opposition repräsentiert sei, vgl. EGMR 6.9.1978 – 5029/71 Rn. 57 – Klass und andere gg. Deutschland. Da das PKGr selbst keine Genehmigung für Beschränkungen erteilt, sondern ein politischer Kontrolleur ist, kann es auf seine Zusammensetzung richtigerweise nicht ankommen.

c. Möglichkeit zur erneuten Wahl

Was die Unabhängigkeit der G 10-Kommission jedoch beeinträchtigt, ist die Tatsache, dass ihre Mitglieder uneingeschränkt wiederholt wählbar sind⁸³: Anders als die Mitglieder des GeKon, deren Wiederwahl explizit „unzulässig“ ist (§ 45 Abs. 1 S. 2 BNDG) oder dem Bundesbeauftragten für Datenschutz, der nur einmalig wiedergewählt werden kann (§ 11 Abs. 3 BDSG), gibt es keine gesetzliche Begrenzung für die Häufigkeit der Mitgliedschaft in der G 10-Kommission. Die Gefahr für die Unabhängigkeit der Mitglieder der G 10-Kommission besteht darin, dass Mitglieder, die ihr Amt länger als eine Wahlperiode ausüben möchten, zwangsläufig darauf achten müssen, bei der parlamentarischen Fraktion, die sie aufgestellt hat, nicht negativ aufzufallen. Ansonsten würden sie ihre Wiederwahl gefährden. Offenbar teilte die Bundesregierung 2021 diese Befürchtung, denn in der Gesetzesbegründung zum Verbot der Wiederwahl von Mitgliedern des GeKon heißt es: „Die Unabhängigkeit der Mitglieder darf nicht durch eine Wiederwahlverpflichtung konterkariert werden.“⁸⁴ Das Problem der Möglichkeit zur erneuten Wahl relativiert sich aber dadurch, dass die Mitgliedschaft in der G 10-Kommission wegen der Ehrenamtlichkeit zumindest aus finanzieller Perspektive unattraktiv ist.

Dass die Mitglieder der G 10-Kommission wiederholt gewählt werden dürfen, liegt daran, dass ihre Amtszeit an die Dauer einer Wahlperiode anknüpft und damit vergleichsweise kurz ist. Da Kontrollen im Nachrichtendienstrecht eine hohe fachliche Expertise und eine lange Einarbeitungszeit erfordern, wäre es nicht angemessen, auf diese eingearbeiteten Fachleute und ihren Sachverstand gleich nach der nächsten Wahl wieder zu verzichten. Außerdem ist es schwierig, so häufig qualifiziertes Personal zu finden. So hat sich auch die Venedig-Kommission bei Nachrichtendienstkontrollleuten für eine längere Amtszeit ausgesprochen:

„The members' tenure can be made longer than the standard electoral period, something which is particularly important as intelligence has, as already mentioned (see above para 90), a relatively long "learning curve".⁸⁵

⁸³ Schwabenbauer, Heimliche Grundrechtseingriffe, S. 352; „(...) angewiesen auf eine Wiederwahl nach vier Jahren durch ein bestimmtes politisches Lager“, Steinke, Verfassungsschutz, S. 64.

⁸⁴ Dt. Bundestag, Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 108.

⁸⁵ Venedig-Kommission, Report 2015, S. 50 Rn. 229.

Die Amtszeit der Mitglieder der G 10-Kommission sollte daher auf acht oder wie die der Mitglieder des GeKon auf zwölf Jahre erhöht und eine Wiederwahl ausgeschlossen werden.

Im Ergebnis beeinträchtigt die Möglichkeit der uneingeschränkten Wiederwahl von Mitgliedern der G 10-Kommission die verfassungsrechtlich vorgegebene „Unabhängigkeit“.

3. Stellung als Parlamentarier und Ehrenamtlichkeit

a. Tätigkeit als Abgeordnete

In manchen Fachgesetzen ist festgelegt, dass die Kommission mit Abgeordneten des Landtages zu besetzen ist.⁸⁶ Demgegenüber sollen der G 10-Kommission anderswo gar keine Abgeordneten angehören.⁸⁷ Überwiegend können die Abgeordneten im Landtag bzw. im Kontrollgremium jedoch frei entscheiden, welche Personen ernannt werden sollen. So wirken in der G 10-Kommission des Bundes aktuell keine Abgeordneten mit⁸⁸, in den Ländern werden jedoch häufig ausschließlich Landtagsabgeordnete damit betraut.⁸⁹

Wenn die Mitglieder (Landtags-)abgeordnete sind, stellt sich die Frage, ob eine „hinreichend wirksame“ Kontrolle vorliegt, da die Arbeit für die G 10-Kommission zusätzlich zur eigentlichen parlamentarischen Tätigkeit wahrgenommen wird.⁹⁰ Bei entsprechender Aufgabenverteilung in der Fraktion ist es jedoch grundsätzlich denkbar, dass eine wirksame Kontrolle gewährleistet werden kann.

⁸⁶ § 1 Abs. 2 S. 2 [AG G 10 RP](#); § 2 Abs. 1 S. 3 [HmbG10AusfG](#); § 2 Abs. 2 S. 2 [AGG10 TH](#), § 2 Abs. 1 [HAGG10](#). In Sachsen sei es parlamentarische Praxis, dass die Mitglieder der Kommission MdL sind, wird auf Nachfrage durch den Landtag erläutert.

⁸⁷ Dies ergebe sich für das Saarland aus einer Zusammenschau von § 2, 3 [G10DGSL](#), erläutert der Geschäftsführer der Kommission auf Anfrage der Autorin. Auch in Bremen existiere eine langjährige Praxis, die G 10-Kommission nicht mit Abgeordneten zu besetzen (Antwort auf Anfrage).

⁸⁸ https://www.bundestag.de/ausschuesse/weitere_gremien/g10_kommission/mitglieder-868160, (abgerufen am 31.8.2024).

⁸⁹ In Schleswig-Holstein und Sachsen entspreche es der Praxis des Landtags, die G 10-Kommission mit Abgeordneten zu besetzen, wird auf Rückfrage von der Kommission erläutert. Auch in Bayern handle es sich der parlamentarischen Praxis folgend seit Jahrzehnten um Abgeordnete. Vgl. zudem: <https://landtag-rlp.de/de/parlament/ausschuesse-und-gremien/sonstige-ausschuesse-kommis/g-10-kommission.htm>, <https://www.landtag-mv.de/landtag/ausschuesse/weitere-gremien/g-10-kommission>, (abgerufen am 31.8.2024).

⁹⁰ Schwabenbauer sieht hierin zudem ein Befangenheitsproblem, weil die Abgeordneten zugleich für die Gesetzgebung zuständig sind, deren Umsetzung sie kontrollieren sollen, *Schwabenbauer*, Heimliche Grundrechtseingriffe, S. 351.

b. Ehrenamtlichkeit der Mitglieder

Gem. § 15 Abs. 1 S. 4 G 10, § 30 Abs. 1 S. 4 VSG NRW und § 3 Abs. 1 S. 7 AGG10-LSA ist die Tätigkeit für die G 10-Kommission explizit ehrenamtlich, auch für die Berliner G 10-Kommission wird auf Rückfrage der Autorin bestätigt, dass es sich um ein Ehrenamt handelt. In den anderen Gesetzen findet man hierzu nichts, wobei teilweise festgelegt ist, dass eine Aufwandsentschädigung zu zahlen oder Reisekosten zu erstatten sind⁹¹. Oft sind in den Haushaltsplänen Aufwandsentschädigungen für die G 10-Kommission eingeplant.⁹² Die genannten Regelungen ergeben nur dann Sinn, wenn es sich um eine ehrenamtliche Tätigkeit handelt.

Dass die G 10-Kommission nicht hauptamtlich kontrolliert, wird zu Recht kritisiert.⁹³ Dass das Bundesverfassungsgericht in seinen Entscheidungen zur G 10-Kommission des Bundes keine Zweifel an der Verfassungsmäßigkeit der ehrenamtlichen Besetzung geäußert hat, ändert nichts daran, dass die Kontrolle nicht hinreichend wirksam ist: Erstens ist die jüngste Entscheidung schon mehr als zwei Jahrzehnte alt (Abhörurteil aus 1999⁹⁴), weshalb die revolutionären technischen Entwicklungen der letzten Jahre nicht berücksichtigt werden konnten. Zweitens kommt erschwerend hinzu, dass die G 10-Kommission in der Zwischenzeit mit umfangreichen zusätzlichen Aufgaben betraut worden ist.⁹⁵ Drittens hat das Gericht bei der Kontrolle der strategischen Ausland-Fernmeldeüberwachung eine Besetzung mit ehrenamtlichen Mitgliedern ausdrücklich als nicht verfassungskonform erachtet, vielmehr sei eine „fachlich kompetente, professionalisierte Kontrolle durch grundsätzlich hauptamtlich tätige Personen

⁹¹ § 3 Abs. 10 [G10DGS](#); § 2 Abs. 6 [G10AGB](#).

⁹² Vgl. z. B. im baden-württembergischen Staatshaushaltsplan 2022, Einzelhaushaltsplan Landtag, S. 16, https://fm.baden-wuerttemberg.de/fileadmin/redaktion/m-fm/intern/Bilder/Haushalt_Finanzen_Steuern/Haushalt_2022/Haushaltsplan_2022/Einzelplan_01_Landtag.pdf (zuletzt abgerufen am 31.8.2024) waren beispielsweise 26,500 Euro veranschlagt; Saarland https://www.saarland.de/Shared-Docs/Downloads/DE/mfw/Haushaltsplan_2023_final/Einzelplan01.pdf?__blob=publication-File&v=1, S. 8 (zuletzt abgerufen am 31.8.2024), veranschlagt sind 2800 Euro.

⁹³ *Gusy*, VerwArch 2015, 437, 449; *Bantlin*, G 10-Kommission, S. 155; „nicht mehr zeitgemäß[e] ehrenamtlich[e] Tätigkeit“, *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 15; *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15; *Bäcker*, Hdb. des Verfassungsrechts, 1715, 1754, Rn. 119, vgl. auch Interview mit Matthias Bäcker, Der Spiegel, 30.4.2022, <https://www.spiegel.de/panorama/justiz/auswuechse-beseitigen-an-denen-niemand-interesse-haben-kann-a-e5e28934-9f8a-4a5e-9065-5905f3f1bf4>; im Kontext der Ausland-Fernmeldeüberwachung BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 287.

⁹⁴ BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95.

⁹⁵ „Der Schutzbereich des Art. 10 GG. ist damit deutlich verlassen; die Kommission mutiert damit in Richtung eines allgemeinen Gremiums für die Einzelfallkontrolle von Spezialbefugnissen der Nachrichtendienste (...)“, *Bartodziej*, Hdb. des Rechts der Nachrichtendienste, 1533, 1591.

sicherzustellen“.⁹⁶ Da die strategische Überwachung und die Telekommunikationsüberwachung in ihrer Eingriffsintensität mit der strategischen Ausland-Fernmeldeüberwachung nahezu vergleichbar sind⁹⁷, kann eine ehrenamtliche Ausgestaltung des Kontrollorgans der strategischen Ausland-Fernmeldeüberwachung nicht verfassungswidrig und die Besetzung der G 10-Kommission mit ehrenamtlichen Mitgliedern zugleich verfassungskonform sein.⁹⁸

Im Ergebnis ist eine rein ehrenamtliche Besetzung der G 10-Kommission nicht „hinreichend wirksam“ und deshalb nicht verfassungskonform. Denkbar wäre, den ehrenamtlichen Mitgliedern hauptamtliche Mitarbeiter zur Verfügung zu stellen, um so insgesamt einen hinreichenden Grad an Professionalisierung zu erreichen.

4. Mehrheitsfindung innerhalb der Kommissionen

Aus vielen Gesetzen oder Geschäftsordnungen ergibt sich, dass die G 10-Kommission ihre Entscheidung mit einfacher Mehrheit der Mitglieder trifft⁹⁹, teilweise ist zudem geregelt, dass im Zweifelsfall die Stimme des Vorsitzenden entscheidend ist¹⁰⁰.

5. Geheimhaltung

Die Sitzungen der G 10-Kommission sind geheim und ihre Mitglieder sind – auch nach dem Ausscheiden aus der Kommission – zur Geheimhaltung verpflichtet.¹⁰¹

Gem. § 3 Abs. 2 Nds. AGG10 sind die Mitglieder, ihre Stellvertreter und die Mitarbeiter der G 10-Kommission zur erweiterten Sicherheitsüberprüfung gem. § 7 Abs. 3 Nds. SÜG verpflichtet. Zuständige Stelle für die Sicherheitsüberprüfung ist grundsätz-

⁹⁶ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 287.

⁹⁷ Vgl. [Teil 2 A. III. 4. b. aa\).](#)

⁹⁸ Im Ergebnis ebenso *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 656.

⁹⁹ § 3 Abs. 5 [GOG 10-Kommission](#); § 30 Abs. 6 [VSG NRW](#); § 3 Abs. 1 S. 5 [Nds. AG G 10](#); § 3 Abs. 3 S. 2 [AG G10 Bremen](#); § 2 Abs. 3 S. 2 [G10AGBbg](#); § 3 Abs. 2 [Sächs AGG10](#); § 5 Abs. 2 S. 3 [GO G10-K Schleswig-Holstein](#); § 3 Abs. 3 [GO G10-K LSA](#); § 4 Abs. 2 S. 1 [GO G10-K BW](#); § 7 Abs. 2 [GO G10-Kommission Thüringen](#), bestätigt auch für Hessen und Bayern.

¹⁰⁰ So in NRW, im Saarland (§ 3 Abs. 3 [G10DGSL](#)), in Berlin (§ 2 Abs. 5 [AG G10 Bln](#)).

¹⁰¹ § 15 Abs. 2 [G 10](#); § 30 Abs. 2 [VSG NRW](#); § 1 [GO G 10-Kommission BW](#); § 5 Abs. 3 [HAGG10](#); § 1 Abs. 4 [G10AG RP](#); § 3 Abs. 4 [G10DGSL](#); § 3 Abs. 3 [Nds. AG G 10](#); § 3 Abs. 4 [AG G10 Bremen](#); § 26a, § 26 Abs. 6 [LVerfSchG SH](#); § 2 Abs. 5 [G10AGBbg](#); § 2 Abs. 6 [AG G10 Bln](#); § 3 Abs. 3 [Sächs AGG10](#); § 2 Abs. 4 [AGG10 TH](#); § 4 Abs. 4 [AGG 10-LSA](#); Art. 2 Abs. 7 [AGG10BY](#); nicht explizit normiert, ergibt sich aber im Umkehrschluss aus der Geheimhaltungsverpflichtung in § 2 Abs. 4 [HmbG10AusfG](#), § 2 Abs. 4 [AG G 10 MV](#).

lich der Geheimschutzbeauftragte des Landtages. Der Gesetzgeber erachtete die erweiterte Sicherheitsüberprüfung als notwendig, da diese Personen „im Rahmen ihrer Kontrolltätigkeit laufend Einblick in als geheim eingestufte Verschlusssachen erhalten“.¹⁰²

Eine vergleichbare Regelung wie in Niedersachsen existiert auch in Sachsen-Anhalt, wobei dort Mitglieder, die Landtagsabgeordnete sind, von der Sicherheitsüberprüfung ausgenommen sind (§ 4 Abs. 2 AG G 10-LSA).

Gem. § 9 Abs. 3 der GO der G 10-Kommission in Thüringen müssen sich auch die Mitglieder der thüringischen G 10-Kommission, die Abgeordnete sind, einer Sicherheitsüberprüfung unterziehen.

V. Distanz

Alle Mitglieder der G 10-Kommissionen sind in ihrer Amtsführung unabhängig und Weisungen nicht unterworfen.¹⁰³ Damit sind sie einerseits unabhängig von den Fraktionen¹⁰⁴ und andererseits an Einzelfallweisungen oder generelle Verwaltungsvorschriften der Exekutive nicht gebunden.¹⁰⁵ Diese Ausgestaltung ist verfassungskonform. Nach konventionsrechtlichen Maßgaben ist insbesondere entscheidend, wer den Kontrolleur ernannt. Da die G 10-Kommissionen von den Parlamenten besetzt werden und der EGMR dies als konventionskonform erachtet hat¹⁰⁶, bestehen auch insoweit keine Bedenken.

Die Geschäftsordnungen unterscheiden sich dahingehend, inwieweit Vertreter aus dem zuständigen Ministerium bei Sitzungen anwesend sein dürfen. In Baden-Württemberg und Sachsen haben der Innenminister und seine Beauftragten zwar das Recht, an Sitzungen teilzunehmen, von Beratungen und Abstimmungen sind sie jedoch ausgeschlossen (§ 5 Abs. 2, 3 GeschO BW, § 4 Abs. 5 GeschO Sachsen). Vereinzelt ist ein Teilnahmerecht bzw. eine Teilnahmepflicht von Vertretern des Innenministeriums normiert, ohne dass eine Regelung dazu getroffen wird, ob das Anwesenheitsrecht der Beamten sich auch auf Abstimmungen erstreckt (§ 3 Abs. 3 GO G 10-Kommission, § 5

¹⁰² Niedersächsischer Landtag, 15. Wahlperiode, Ds. 15/270, Gesetzesentwurf zur Änderung verfassungs- und geheimschutzrechtlicher Vorschriften vom 18.6.2003, S. 34, https://www.landtag-niedersachsen.de/Drucksachen/Drucksachen_15_2500/0001-0500/15-0270.pdf (abgerufen am 31.8.2024).

¹⁰³ § 15 Abs. 1 S. 3 G 10; § 30 Abs. 1 S. 3 VSG NRW; § 2 Abs. 5 S. 2 AG G 10 BW; § 5 Abs. 1 S. 3 HAGG 10; § 1 Abs. 3 G 10 AG RP; § 3 Abs. 1 S. 3 G 10 DGS L; § 3 Abs. 1 S. 6 Nds. AG G 10; § 2 Abs. 1 S. 4 Hmb G 10 Ausf G; § 3 Abs. 3 S. 2 AG G 10 Bremen; § 26a Abs. 2 S. 4 LVerfSchG SH; § 2 Abs. 3 S. 2 AG G 10 MV; § 2 Abs. 3 S. 1 G 10 AG Bbg; § 2 Abs. 4 S. 2 AG G 10 Bln; § 3 Abs. 1 S. 2 Sächs AGG 10; § 2 Abs. 3 AGG 10 TH; § 4 Abs. 3 AG G 10-LSA; Art. 2 Abs. 6 S. 2 AGG 10 BY.

¹⁰⁴ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 22.

¹⁰⁵ Gusy, Grundrechte und Verfassungsschutz, S. 35 f.

¹⁰⁶ Vgl. Teil 2 B. I. 4. a.

Abs. 2 S. 2 GeschO SH). Da eine Teilnahme von Vertretern der Exekutive an der Beratung und der Abstimmung die Unabhängigkeit der G 10-Kommission gefährdet, sollte deren Teilnahmerecht aus verfassungsrechtlichen Gründen beschränkt werden.

VI. Modalitäten

In welcher Modalität die Kontrolle erfolgt, hängt von der jeweiligen Aufgabe ab (1.). Wie oft die Kommission tagt, ist sehr unterschiedlich (2.).

1. Differenzierung nach der Aufgabe

Grundsätzlich muss zwischen der Funktion der G 10-Kommission als Vorabkontrolleur und derjenigen als Datenschutzkontrolleur unterschieden werden.

Die Vorabkontrolle erfolgt für jede einzelne Beschränkung, da die Beschränkung von der Genehmigung abhängt. Abgesehen davon wird die Kommission über jede Benachrichtigung an Betroffene bzw. Gründe für die Zurückstellung einer Benachrichtigung unterrichtet und ist insoweit dauerhaft eingebunden. Die Datenschutzkontrolle erfolgt nach der Rechtsprechung des Bundesverfassungsgerichts grundsätzlich stichprobenartig. Aus dem G 10 und den Ausführungsgesetzen der Länder ergibt sich nicht, dass die G 10-Kommission innerhalb ihres Zuständigkeitsbereichs jede Verarbeitung kontrolliert, weshalb in der Praxis von einer solchen stichprobenartigen Kontrolle auszugehen ist.

2. Sitzungsrhythmus

a. Bundesebene

Die G 10-Kommission des Bundes tagt mindestens einmal monatlich (§ 15 Abs. 4 G 10).

Während der monatlichen Sitzung muss die G 10-Kommission des Bundes „mehrere hundert Fälle bearbeiten“, was dazu führt, dass pro Fall „nur fünf bis dreißig Minuten zur Verfügung stehen“. Auch wenn die Fälle bereits aufbereitet und die Kommissionsmitglieder eingearbeitet sind, ist davon auszugehen, dass eine so kurze Zeitspanne nicht ausreichend ist, um eine wirksame Kontrolle sicherzustellen.¹⁰⁷

¹⁰⁷ Bantlin, G 10-Kommission, S. 163.

b. Länderebene

In Nordrhein-Westfalen, Baden-Württemberg, Schleswig-Holstein und Sachsen findet grundsätzlich alle drei Monate eine Sitzung statt, wobei bei Bedarf Sondersitzungen einberufen werden können.¹⁰⁸

Die G 10-Kommissionen bzw. ihre Mitarbeiter in Bremen, Mecklenburg-Vorpommern und Bayern haben mitgeteilt, dass die Sitzungen keinem festen Rhythmus folgen. In Hessen würden die Sitzungen „regelmäßig“ erfolgen, weil der zuständige Minister gem. § 2 Abs. 1 HAGG10 „unverzüglich“ über Beschränkungsmaßnahmen unterrichten müsse. In Thüringen wird die Kommission von ihrem Vorsitzenden anlassbezogen mit einer Einberufungsfrist von mindestens fünf Tagen schriftlich einberufen, wenn eine Unterrichtungspflicht nach dem AGG10 besteht (§ 6 Abs. 1 GO).

Die G 10-Kommissionen in Rheinland-Pfalz und Berlin haben eine Aussage zum Sitzungsrhythmus schlichtweg verweigert, mit Verweis auf Geheimhaltungserfordernisse. Das überzeugt nicht, denn die Häufigkeit der Sitzungen ist nicht geheimhaltungsbedürftig- die Inhalte der Besprechungen sind es.

In den übrigen fünf Ländern, in Sachsen-Anhalt, Brandenburg, Niedersachsen, Hamburg und dem Saarland, ist der Sitzungsrhythmus nicht bekannt, weil weder Anfragen beantwortet wurden noch Geschäftsordnungen zugänglich waren.

Anders als auf der Bundesebene lässt sich nicht beurteilen, ob die Anzahl der Sitzungen ausreichend ist, um wirksame Kontrollen sicherzustellen, weil es keine Zahlen oder verlässlichen Schätzungen dazu gibt, wie viele Maßnahmen die Landesverfassungsschutzbehörden beantragen. Es ist jedoch davon auszugehen, dass die Anzahl der Anordnungen jedenfalls in Bundesländern mit vergleichsweise kleinen Landesämtern für Verfassungsschutz deutlich geringer sein wird und dass die Sitzungen daher nicht ebenso häufig erfolgen müssen wie auf der Bundesebene.

VII. Initiative

Bei der Vorabkontrolle durch die G 10-Kommission und die Entscheidung über die Mitteilung an Betroffene geht die Initiative grundsätzlich von der Exekutive aus, da die G 10-Kommission zunächst informiert werden muss (vgl. § 15 Abs. 6 G 10). Zusätzlich steht der G 10-Kommission ein Initiativrecht zu. Sie kann „von sich aus von Amts wegen“ sowohl die Erhebung als auch die sonstige Verarbeitung personenbezogener Daten kontrollieren.¹⁰⁹

¹⁰⁸ § 30 Abs. 1 S. 6 [VSG NRW](#), bezüglich der anderen Länder ergibt sich dies aus den Antworten der G 10-Kommissionen auf die Frage nach dem Sitzungsrhythmus, der nicht normiert ist.

¹⁰⁹ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 35, 44.

Da auf der Landesebene ebenfalls normiert ist, dass die Kommission „von Amts wegen“ tätig werden kann, hat sie auch dort ein Kontrollinitiativrecht. Darüber hinaus wird die Kommission dann tätig, wenn Betroffene sich an sie wenden.

VIII. Kontrollmittel zur Informationsgewinnung

Die G 10-Kommissionen können sich auf vielfältige Weise über den Ist-Zustand informieren. Ihre Rechte sind an den Kontrollgegenstand gebunden.¹¹⁰

1. Unterrichtungspflicht

Zunächst muss das zuständige Innenministerium die G 10-Kommissionen über Beschränkungen nach dem G 10 und über die Zurückstellung von Benachrichtigungen Betroffener unterrichten.¹¹¹ Diese Unterrichtungspflicht muss sich auch auf sonstige Maßnahmen erstrecken, für deren Genehmigung die G 10-Kommission zuständig ist.

2. Auskunfts-, Einsichts- und Zutrittsrecht

Darüber hinaus stehen der Kommission bestimmte Kontrollbefugnisse zu.

a. Umfang

Auf der Bundesebene und in den meisten Bundesländern ist ihr „1. Auskunft zu ihren Fragen zu erteilen und 2. Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Beschränkungsmaßnahme stehen und 3. jederzeit Zutritt in alle Diensträume zu gewähren“.¹¹²

In weiteren drei Bundesländern wird der Kommission zwar ein Zutrittsrecht eingeräumt, das aber nicht jederzeit geltend gemacht werden kann.¹¹³

¹¹⁰ Gusy, Grundrechte und Verfassungsschutz, S. 46.

¹¹¹ § 15 Abs. 6, 7 G 10; § 2 Abs. 2, 3 [AG G 10 BW](#); § 2 Abs. 1, § 4 Abs. 2, 3 [HAGG10](#); § 3 Abs. 1, § 4 [G10AG RP](#); § 2 Abs. 2, § 3 Abs. 7, 8 [G10DGS](#); § 2 Abs. 2 [Nds. AG G 10](#); § 1 Abs. 2 [HmbG10AusfG](#); § 2, § 3 Abs. 2 [AG G10 Bremen](#); § 26a Abs. 1 S. 2 [LVerfSchG SH](#); § 15 Abs. 6, 7 G 10; § 2 Abs. 1, 2 [AG G 10 MV](#); § 3 Abs. 1, 2 [G10AGBbg](#); § 2 Abs. 1, 3 [AG G10 Bln](#); § 2 Abs. 1, 2 [Sächs AGG10](#); § 3 Abs. 1, § 4 [AGG10 TH](#); § 3, § 6 Abs. 1 [AG G 10-LSA](#); Art. 2 Abs. 1, 4 [AGG10BY](#); nicht ausdrücklich normiert in § 30 Abs. 5 [VSG NRW](#).

¹¹² § 15 Abs. 5 G 10; § 30 Abs. 5 S. 3 [VSG NRW](#); § 2 Abs. 4 S. 2 [AG G 10 BW](#); § 4 Abs. 1 S. 3 [HAGG10](#); § 2 Abs. 3 S. 2 [G10AG RP](#); § 3 Abs. 6 S. 3 [G10DGS](#); § 4 Abs. 2 S. 2 [Nds. AG G 10](#); § 3 Abs. 1 S. 6 [AG G10 Bremen](#); § 26a Abs. 1 S. 2 [LVerfSchG SH](#); § 15 Abs. 5 G 10; § 2 Abs. 1 S. 7 [AG G 10 MV](#); § 2 Abs. 2 S. 2 [AG G10 Bln](#); § 2 Abs. 2 S. 2 [Sächs AGG10](#); § 3 Abs. 2 S. 2 [AGG10 TH](#).

¹¹³ § 1 Abs. 5 S. 2 Nr. 3 [HmbG10AusfG](#); § 5 Abs. 2 S. 2 Nr. 3 [AG G 10-LSA](#); Art. 2 Abs. 5 Nr. 3 [AGG10BY](#).

In Brandenburg sind keine dieser Rechte und auch keine vergleichbaren normiert, sodass nicht davon ausgegangen werden kann, dass die G 10-Kommission dort umfassend informiert ist. Zumindest ein Einsichtsrecht wäre für eine verfassungskonforme und konventionskonforme Ausgestaltung jedoch notwendig.¹¹⁴

Das Auskunftsrecht ermöglicht nicht nur die Befragung von Personen, welche die Behördenleitung ausgewählt hat, sondern von allen mit dem konkreten Vorgang befassten Mitarbeitern des Nachrichtendienstes.¹¹⁵ Darüber hinaus gilt: Wenn die G 10-Kommissionen Zutritt in Diensträume der Nachrichtendienste oder die mit Beschränkungsmaßnahmen betrauten Ministerien begehren, hat er zu erfolgen.¹¹⁶

Gegenüber den G 10-Kommissionen kann sich die Exekutive auf Geheimhaltungserfordernisse nicht berufen.¹¹⁷

b. Anspruchsberechtigte

Vergleicht man, wem diese Rechte zustehen, zeigen sich drei Regelungsmodelle: Erstens gibt es Modelle, bei denen sich ausschließlich die G 10-Kommission darauf berufen kann.¹¹⁸ In Sachsen kann die G 10-Kommission hierbei ihre Mitarbeiter hinzuziehen.¹¹⁹

Zweitens werden neben der G 10-Kommission auch die Mitarbeiter der Kommission berechtigt.¹²⁰

Das dritte Modell entspricht dem zweiten Modell und sieht ergänzend vor, dass einzelne Mitglieder beauftragt werden können, im Namen der G 10-Kommission von den Rechten Gebrauch zu machen.¹²¹

¹¹⁴ Das BVerfG betont, dass eine umfassende Protokollierung die Voraussetzung von Kontrollen darstellt, vgl. [Teil 2 A. III. 1. a. gg.](#) Nur wenn der Kontrolleur in diese Protokolle auch Einsicht nehmen kann, erfüllt die Dokumentation ihren Zweck; zur Rechtsprechung des EGMR, vgl. [Teil 2 B. I. 4. a. aa.](#)

¹¹⁵ Gusy, Grundrechte und Verfassungsschutz, S. 49, der diese Schlussfolgerung u.a. mit der Notwendigkeit einer der richterlichen Kontrolle „gleichwertigen“ Ausgestaltung begründet.

¹¹⁶ Das Recht erstreckt sich auf alle Räume, in denen die Kommission wichtige Informationen gewinnen könnte, Gusy, Grundrechte und Verfassungsschutz, S. 51; die Rechte können auch gegenüber anderen Stellen geltend gemacht werden, die G 10-Daten verarbeiten, Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 50.

¹¹⁷ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 48; „Ihr gegenüber gibt es insbesondere weder eine Weigerung, irgendwelche Akten und Unterlagen vorzulegen (wie z.B. in § 99 VwGO), noch eine Dienstverschwiegenheiten von Angehörigen des öffentlichen Dienstes“, Arndt, G 10-Verfahren, 43, 57.

¹¹⁸ § 3 Abs. 6 S. 3 [G10DGS](#); § 3 Abs. 1 S. 6 [AG G10 Bremen](#); § 2 Abs. 2 S. 2 [Sächs AGG10](#); Art. 2 Abs. 5 S. 1 [AGG10BY](#); „auf Antrag mindestens eines ihrer Mitglieder“ in § 1 Abs. 5 S. 2 [HmbG10AusfG](#).

¹¹⁹ § 2 Abs. 2 S. 3 [Sächs AGG10](#).

¹²⁰ § 15 Abs. 5 G 10; § 30 Abs. 5 S. 3 [VSG NRW](#); § 2 Abs. 4 S. 2 [AG G 10 BW](#); § 2 Abs. 3 S. 2 [G10AG RP](#); § 4 Abs. 1 S. 3 [HAGG10](#); § 26a Abs. 1 S. 2 [LVerfSchG SH](#); § 15 Abs. 5 G 10; § 2 Abs. 1 S. 7 [AG G 10 MV](#).

¹²¹ § 4 Abs. 2 S. 2 [Nds. AG G 10](#); § 2 Abs. 2 S. 2 [AG G10 Bln](#); § 3 Abs. 2 S. 2 [AGG10 TH](#); § 5 Abs. 2 S. 2 [AG G 10-LSA](#).

Anders als bei vergleichbaren Rechten der Parlamentarischen Kontrollgremien teilweise üblich¹²², sind diese Rechte der Kommission grundsätzlich nur als Einheit verliehen, soweit sie nicht nach dem dritten Modell einzelne Mitglieder dazu berechtigen. Das bedeutet, einzelne Mitglieder können sich ohne einen entsprechenden Beschluss der Kommission nicht darauf berufen. Diese Folgerung liegt nach dem Wortlaut nahe („Der Kommission (...)“) und wurde aus der Praxis mehrfach bestätigt.¹²³

c. Einschränkungen der Rechte

Regelungen, die die Einsichtnahme in Dokumente begrenzen, müssen dahingehend bewertet werden, ob die Kontrolle wirksam bleibt. Zumindest diskussionsbedürftig sind insoweit Normen, wonach die Einsichtnahme der G 10-Kommission durch eine Entscheidung des Innenministeriums auf den Zeitraum „während der Sitzungen“ begrenzt werden kann (§ 5 Abs. 4 der GO der G 10-Kommission in Baden-Württemberg). Da die zu sichtenden Dokumente sehr umfangreich sein können, kann nicht davon ausgegangen werden, dass dieser knappe Zeitraum stets ausreichend dafür sein wird, den Ist-Zustand zu verstehen.

IX. Kontrollerggebnisfolgen

Der Vorabkontrolleur entscheidet darüber, ob die Maßnahme erfolgen kann oder nicht, die Exekutive muss dessen Vorgaben umsetzen.¹²⁴ So ist es auch bei der Vorabkontrolle durch die G 10-Kommission, da der Nachrichtendienst an ihre Entscheidungen gebunden ist.¹²⁵

Demgegenüber ist für die Datenschutzkontrolle durch die G 10-Kommission verfassungsrechtlich keine vergleichbar detaillierte Vorgabe etabliert worden, sie muss „wirksam sein“¹²⁶. Aus dem G 10 ergeben sich insoweit weder ein Beanstandungsrecht¹²⁷ noch sonstige Abhilfebefugnisse.

¹²² § 3 Abs. 2 PKGrG; § 34 Abs. 1 [LVerfSchG RP](#); § 4 Abs. 2 [HEKontrollG](#); § 26 Abs. 3 Nr. 1 [Hmb-VerfSchG](#); § 35 Abs. 2 [VSG Bln](#); vgl. *Michel*, GSZ 2021, 197, 202.

¹²³ Bestätigt wurde dies von den Zuständigen in NRW, Baden-Württemberg, Bremen und Mecklenburg-Vorpommern.

¹²⁴ Vgl. [Teil 2 A. III. 1. a. hh](#)), [Teil 2 A. III. 1. b. hh](#)), [Teil 2 B. I. 4. a. aa](#)).

¹²⁵ § 3 Abs. 1 [HAGG10](#); § 2 Abs. 4 [G10AG RP](#); § 4 Abs. 5, 6 [Nds. AG G 10](#); § 1 Abs. 3 [HmbG10AusfG](#); § 2 Abs. 1, 2 [AG G 10 MV](#); § 3 Abs. 1 [G10AGBbg](#); § 2 Abs. 3 [AG G10 Bln](#); § 2 Abs. 1 [Sächs AGG10](#); § 3 Abs. 1, § 4 [AGG10 TH](#); § 5 Abs. 1 [AG G 10-LSA](#); Art. 2 Abs. 4 [AGG10BY](#). Soweit die Kontrollerggebnisfolgen nicht konkretisiert wurden, lässt sich die Verbindlichkeit der Kontrollerggebnisfolge daraus ableiten, dass die Kommission überall über die „Zulässigkeit und Notwendigkeit“ der Maßnahme „entscheidet“.

¹²⁶ Vgl. [Teil 2 A. III. 1. a. hh](#)).

¹²⁷ *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 17.

Dass für die laufende Datenschutzkontrolle keine Kontrollerggebnisfolge festgelegt wurde, ist ein Regelungsdefizit, dem schnellstmöglich abgeholfen werden sollte. Um die Wirksamkeit der Kontrolle sicherzustellen, sollte der G 10-Kommission auch bei der Datenschutzkontrolle ein abschließendes Entscheidungsrecht verliehen werden. In der Praxis kann dem Regelungsdefizit dadurch abgeholfen werden, dass die G 10-Kommission androht, eine Genehmigung nicht zu verlängern oder zukünftig zu verweigern, falls der Nachrichtendienst den rechtswidrigen Zustand nicht behebt.

X. Fachkompetenz und Ressourcen

In der Frage, welche Fachkompetenz für einen Kontrolleur vorgeschrieben ist und wie viel Unterstützung er erhält, unterscheiden sich die Gesetze zum Teil deutlich.

1. Fachkompetenz

Das Bundesverfassungsgericht hat festgestellt, dass der Vorabkontrolleur über die „notwendige Sach- und Rechtskunde“ verfügen muss.¹²⁸

Gem. § 15 Abs. 1 S. 2 G 10 müssen mindestens drei Mitglieder und drei stellvertretende Mitglieder der G 10-Kommission die Befähigung zum Richteramt besitzen. Gemäß den meisten Fachgesetzen auf der Länderebene muss mindestens eine Person, der Vorsitzende der Kommission, Volljurist sein.¹²⁹ Damit dürfte die durch das Bundesverfassungsgericht geforderte Voraussetzung der „notwendigen Rechtskunde“ erfüllt sein.¹³⁰

Darüber, welche Sachkunde innerhalb der G 10-Kommission vorhanden sein muss, schweigen die Gesetze aus gutem Grund. Denn würden zusätzlich technische und nachrichtendienstliche Vorkenntnisse gesetzlich vorgeschrieben, würde dies die Besetzung der Kommissionen vor allem auf der Landesebene zu sehr erschweren bzw. unmöglich machen.

¹²⁸ Vgl. [Teil 2 A. III. 1. a. ii\).](#)

¹²⁹ § 30 Abs. 1 S. 2 [VSG NRW](#); § 2 Abs. 5 S. 1 [AG G 10 BW](#); § 5 Abs. 1 S. 2 [HAGG10](#); § 1 Abs. 2 S. 1 [G10AG RP](#); § 3 Abs. 1 S. 2 [G10DGS](#); § 3 Abs. 1 S. 1 [Nds. AG G 10](#); § 2 Abs. 1 S. 2 [HmbG10AusfG](#), wobei ausreichend ist, wenn ein Mitglied Volljurist ist; § 3 Abs. 3 S. 1 [AG G10 Bremen](#); § 26 a Abs. 2 S. 1 [LVerfSchG SH](#); § 2 Abs. 3 S. 1 [AG G 10 MV](#); § 2 Abs. 1 S. 3 [G10AGBbg](#); § 2 Abs. 4 S. 1 [AG G10 Bln](#); § 3 Abs. 1 S. 1 [Sächs AGG10](#); § 2 Abs. 2 S. 1 [AGG10 TH](#); § 4 Abs. 1 S. 2 [AG G 10-LSA](#); Art. 2 Abs. 6 S. 1 [AGG10BY](#); erachtet die Besetzung mit juristischen Laien als „nicht zulässig“, *Schwabenbauer*, Heimliche Grundrechtseingriffe, S. 348.

¹³⁰ Andere Ansicht Graulich, der u.a. wegen „nicht notwendig professionell vorgebildeten Mitgliedern der Kontrollgremien“ die „Kontrolldichte“ verneint, *Graulich*, Justizgewährung und Geheimdienste, 143, 160.

2. Ressourcen

In der Frage, welche Ressourcen die G 10-Kommission haben soll, unterscheiden sich die Gesetze erheblich.

a. „Notwendige“ Personal- und Sachausstattung

Gem. § 15 Abs. 3 S. 1 G 10 ist der Kommission die „für die Erfüllung ihrer Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen“. Diese Formulierung wurde in acht Landesgesetze übernommen.¹³¹

Gem. § 3 Abs. 1 G10DG SL sind „die erforderlichen Mittel“ im Einzelplan des saarländischen Landtags gesondert auszuweisen, gem. § 2 Abs. 7 S. 2 BbgVerfSchG ist der brandenburgischen G 10-Kommission die „notwendige Sachausstattung“ zur Verfügung zu stellen¹³². Der hessischen G 10-Kommission stehen Mitarbeiter zur Verfügung (§ 4 Abs. 1 S. 3 HAGG10), wie viele, möchte die Kommission jedoch nicht mitteilen.¹³³

Demgegenüber enthalten fünf Gesetze keinerlei Vorgaben zur Ausstattung der Kommission.¹³⁴ Ein Vertreter des baden-württembergischen Landtags hat jedoch erläutert, dass der Landtag von Baden-Württemberg „die erforderliche Sachausstattung (insbesondere Stand-Alone-Laptop, Stand-Alone-Drucker, VS-tauglicher Aktenvernichter und Panzerschrank) stellt“. Es ist denkbar, dass in den restlichen vier Bundesländern, die keine gesetzliche Regelung dazu treffen, entsprechend dem baden-württembergischen Beispiel in der Praxis trotzdem eine entsprechende Sachausstattung vorgesehen ist.

In der Praxis wird § 15 Abs. 3 S. 1 G 10 so umgesetzt, dass das zuständige Sekretariat in der Bundestagsverwaltung „die monatlichen Sitzungen effektiv vorbereitet, indem sich dessen Mitglieder in die zur Beratung anstehenden Fälle vollinhaltlich einarbeiten und eine – jedoch für die Kommission keineswegs bindende – Vorprüfung der Sachverhalte in tatsächlicher und rechtlicher Hinsicht vornehmen“.¹³⁵

b. Geschäftsstellen

Die Antworten auf Anfragen an die G 10-Kommissionen und der Einblick in die GO haben gezeigt, dass in der Praxis häufig eine Geschäftsstelle beim Landtag eingerichtet

¹³¹ § 30 Abs. 3 S. 1 [VSG NRW](#); § 1 Abs. 6 [G10AG RP](#); § 2 Abs. 2 [HmbG10AusfG](#); § 2 Abs. 1 S. 5 [AG G 10 MV](#); § 2 Abs. 7 S. 1 [AG G10 Bln](#); § 3 Abs. 4 [Sächs AGG10](#); § 2 Abs. 5 [AGG10 TH](#); § 4 Abs. 6 S. 1 [AG G 10-LSA](#).

¹³² Als Personal ist der Ständige Bevollmächtigte vorgesehen, dazu s.u. [Teil 3 B. X. 2. f.](#)

¹³³ So lautete die Antwort auf eine Anfrage der Autorin v. 29.3.2023.

¹³⁴ BW, wobei in § 2 Abs. 4 [AG G 10 BW](#) „Mitarbeiter“ erwähnt werden; Nds; Bremen; SH; BY.

¹³⁵ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 29; § 3 Abs. 2 [GO G 10-Kommission](#).

ist, die die G 10-Kommission unterstützt.¹³⁶ Teilweise wird der Stellenanteil dafür explizit im Einzelhaushaltsplan des Landtags ausgewiesen.¹³⁷ Weil der baden-württembergische Gesetzgeber die im Haushaltsplan aufgeführten Kosten der G 10-Kommission erläutert, konnte festgestellt werden, dass der Geschäftsführer und die Assistenz der Geschäftsführung dort lediglich ehrenamtlich tätig sind.¹³⁸ Wie schon bei den Mitgliedern der G 10-Kommission stellt sich auch hier die Frage, inwieweit eine professionelle Kontrolle durch ehrenamtliche Arbeit realisiert werden kann.¹³⁹

Eine frei zugängliche GO der G 10-Kommission Sachsen-Anhalts aus 2014 regelt, dass die Geschäftsstelle beim Ministerium für Inneres und Sport eingerichtet wird (§ 2 GO). Darüber hinaus soll der Geschäftsführer der Kommission vom Ministerium für Inneres und für Sport bestellt werden. Da die Arbeit der Geschäftsstelle die Kommission beeinflusst, ist fraglich, ob hier die Unabhängigkeit der G 10-Kommission gewahrt ist. Dafür spricht, dass der Geschäftsführer nur an Weisungen des Kommissionsvorsitzenden gebunden sein soll (§ 2 Abs. 2). Andererseits verstärkt die räumliche Nähe zum Kontrollierten und dessen Stellung als Dienstherr die Gefahr einer Fraternisierung zwischen dem Kontrolleur und dem Kontrollierten („agency capture“¹⁴⁰). Falls die für diese Arbeit nicht bereitgestellte GO in Sachsen-Anhalt zwischenzeitlich unverändert geblieben ist, sollte sie so angepasst werden, dass die Geschäftsstelle nicht beim Innenministerium angesiedelt ist, weil die höherrangigen Vorgaben nur bei einer unabhängigen Ausgestaltung erfüllt sind.

¹³⁶ § 9 Abs. 1 GO BW: „Die Geschäftsstelle der Kommission wird bei der Verwaltung des Landtags eingerichtet. Sie wird von einem Geschäftsführer geleitet, der vom Landtagspräsidenten im Einvernehmen mit der Kommission bestellt wird.“; § 2 Abs. 3 GO G10 Sachsen: „Die Aufgaben der Geschäftsstelle nehmen die hierfür bestellten Bediensteten der Landtagsverwaltung wahr.“; § 2 Abs. 1 GO G 10 SH: „Die laufenden Geschäfte der Kommission werden durch eine Geschäftsführerin oder einen Geschäftsführer erledigt.“; § 2 GO AGG10 Bremen: „Zur Erfüllung ihrer Aufgaben wird bei der Kommission eine Geschäftsstelle eingerichtet“; § 10 Abs. 1 GO Thüringen: „Die Kommission wird bei der Wahrnehmung ihrer Aufgaben durch einen Beamten der Landtagsverwaltung, der die Befähigung zum Richteramt besitzt (ständiger Geschäftsführer), den stellvertretenden Geschäftsführer und weitere Bedienstete der Landtagsverwaltung unterstützt. Diese bilden die Geschäftsstelle der Kommissionen“.

¹³⁷ Im Haushaltsplan des Abgeordnetenhauses in Berlin wird eine halbe Stelle eines Regierungsdirektors und eine halbe Stelle eines Beamten im mittleren Dienst „zur Wahrnehmung der Aufgaben der G 10-Kommission vorgesehen“, Haushaltsplan von Berlin für die Haushaltsjahre 2022/2023, Band 2, Einzelpläne 01, 02, 20, 21, 22, S. 21 f.; vgl. auch Baden-Württemberg, Staatshaushaltsplan für 2022, Einzelplan 01 Landtag, S. 16.

¹³⁸ Vgl. auch Baden-Württemberg, Staatshaushaltsplan für 2022, Einzelplan 01 Landtag, S. 16: Für den Geschäftsführer ist eine Aufwandsentschädigung von 300 Euro monatlich und für die Assistenz eine Aufwandsentschädigung von 150 Euro monatlich veranschlagt.

¹³⁹ Vgl. [Teil 3 B. IV. 3. b.](#)

¹⁴⁰ Cameron, National Security, S. 167; vgl. [Teil 1 A. III. 11.](#)

c. Mitarbeiter mit technischem Sachverstand

Die Beschränkungen nach dem G 10 und insbesondere die strategische Überwachung setzen für Laien schwer erfassbare, komplexe technische Abläufe voraus, für deren Verständnis technische Expertise erforderlich ist.¹⁴¹ Daher legen einige Gesetze sinnvollerweise fest, dass der G 10-Kommission „Mitarbeiter mit technischem Sachverstand zur Verfügung zu stellen sind“.¹⁴²

d. Rechte der Mitarbeiter

Auf der Bundesebene und in elf Ländern werden den Mitarbeitern der G 10-Kommission dieselben Rechte verliehen, auf die sich auch die Kommission berufen kann: Ihnen stehen Auskunfts-, Akteneinsichts- und Zutrittsrechte zu.¹⁴³

e. Einbindung des Bundes- oder Landesdatenschutzbeauftragten

Die meisten Fachgesetze verleihen der G 10-Kommission das Recht, dem Bundes- oder Landesbeauftragten für Datenschutz „Gelegenheit zur Stellungnahme in Fragen des Datenschutzes“ zu geben.¹⁴⁴ Andere Regelungen sehen vor, dass die Kommission den Landesbeauftragten ersuchen kann, „die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.“¹⁴⁵ Teilweise wurde den Datenschutzbeauftragten – wie der Kommission (und ihren Mitgliedern) – ein Auskunftsanspruch und ein Recht auf Einsicht in Dokumente, Datenverarbeitungssysteme und das Recht auf Zugang zu Räumlichkeiten des Kontrollierten verliehen.¹⁴⁶

¹⁴¹ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 31.

¹⁴² § 15 Abs. 3 S. 2 G 10; § 30 Abs. 3 S. 2 VSG NRW; § 1 Abs. 6 S. 2 G10AG RP; § 2 Abs. 1 S. 6 AG G 10 MV; § 2 Abs. 7 S. 2 AG G10 Bln; § 4 Abs. 6 S. 2 AG G 10-LSA.

¹⁴³ § 15 Abs. 5 G 10; § 30 Abs. 5 S. 3 VSG NRW; § 2 Abs. 4 S. 2 AG G 10 BW; § 4 Abs. 1 S. 3 HAGG10; § 2 Abs. 3 S. 2 G10AG RP; § 4 Abs. 2 S. 2 Nds. AG G 10; 26a Abs. 1 S. 2 LVerfSchG SH; § 15 Abs. 5 G 10; § 2 Abs. 1 S. 7 AG G 10 MV; § 2 Abs. 2 S. 2 AG G10 Bln; § 2 Abs. 2 S. 3 Sächs AGG10 („Sie kann hierzu Mitarbeiter der Kommission hinzuziehen“); § 3 Abs. 2 S. 2 AGG10 TH; § 5 Abs. 2 S. 2 AG G 10-LSA.

¹⁴⁴ § 15 Abs. 5 G 10; § 30 Abs. 5 S. 4 VSG NRW; § 2 Abs. 4 S. 3 AG G 10 BW; § 4 Abs. 1 S. 4 HAGG10; § 3 Abs. 6 S. 4 G10DGSL; § 3 Abs. 1 S. 6 AG G10 Bremen; § 26a Abs. 1 S. 2 LVerfSchG SH; § 15 Abs. 5 G 10; § 3 Abs. 2 AG G 10 MV; § 3 Abs. 1 S. 6 G10AGBbg; § 2 Abs. 2 S. 3 AG G10 Bln; § 2 Abs. 2 S. 4 Sächs AGG10; § 5 Abs. 3 S. 1 AG G 10-LSA.

¹⁴⁵ § 6 Abs. 2 G10AG RP; § 4 Abs. 3 Nds. AG G 10; § 3 Abs. 3 AGG10 TH; ähnlich § 2 Abs. 2 S. 3, 4 AG G10 Bln.

¹⁴⁶ § 4 Abs. 2 S. 2. Nds. AG G 10; § 3 Abs. 2 S. 2 AGG10 TH.

f. Beauftragung des Ständigen Bevollmächtigten

Gem. § 2 Abs. 6 S. 1 G10AGBbg werden die Sitzungen der G 10-Kommission „inhaltlich und organisatorisch“ von dem Ständigen Bevollmächtigten betreut. Der Ständige Bevollmächtigte ist ein Beamter mit der Befähigung zum Richteramt, der das brandenburgische PKGr unterstützt, indem er Sitzungen vorbereitet und im Auftrag des Gremiums „regelmäßige oder einzelfallbezogene Untersuchungen“ vornimmt (§ 25a, b BbgVerfSchG). Auf der Grundlage von § 3 Abs. 1 S. 6 G10AGBbg darf die G 10-Kommission ihn gem. § 25b BbgVerfSchG damit beauftragen, „eine fachliche Stellungnahme zu einer Beschränkungsmaßnahme abzugeben“. Dass die Arbeit der brandenburgischen G 10-Kommission mit dem Ständigen Bevollmächtigten von einem Volljuristen unterstützt wird, der hauptberuflich für die Nachrichtendienstkontrolle zuständig ist, spricht dafür, dass der Professionalisierungsgrad der G 10-Kommission in Brandenburg insgesamt hoch ist.

XI. Kontrollniveau

Teilweise enthalten die Fachgesetze Regelungen, wonach die G 10-Kommission und das PKGr sich zu „allgemeinen Angelegenheiten“ austauschen¹⁴⁷ oder die G 10-Kommission das jeweilige PKGr über Beschlüsse¹⁴⁸ informiert. Auf der Bundesebene ist auch mit dem UKRat ein „allgemeiner“ Austausch vorgesehen (§ 58 Abs. 3 BNDG). „Allgemein“ ist der Austausch deshalb, weil über konkrete Maßnahmen nicht diskutiert werden darf.¹⁴⁹

XII. Barrieren

Möglichen Kontrollbarrieren wird insoweit begegnet, als der G 10-Kommission Rechte verliehen wurden, die uneingeschränkt gelten.¹⁵⁰

1. Ressourcenbarrieren

In den Gesetzen, die normieren, dass der Kommission die „notwendige Personal und Sachausstattung“ zur Verfügung gestellt werden muss¹⁵¹, ist das Risiko von Ressourcenbarrieren minimiert worden. In den anderen Ländern drohen insoweit Kontrollbarrieren.

¹⁴⁷ § 15 Abs. 8 G 10; § 2 Abs. 6 [HmbG10AusfG](#).

¹⁴⁸ § 4 Abs. 1 S. 6 AGG10-LSA.

¹⁴⁹ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 66.

¹⁵⁰ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 48.

¹⁵¹ Vgl. [Teil 3 B. X. 2.](#)

2. *Third Party Rule*-Einwand

Obwohl die Kontrollmittel der G 10-Kommission grundsätzlich unbeschränkt gelten¹⁵², verweigert die Bundesregierung Kontrollbegehren der G 10-Kommission mitunter unter Verweis auf das Staatswohl bzw. die *Third Party Rule*¹⁵³.¹⁵⁴ So hat sich die Bundesregierung beispielsweise¹⁵⁵ geweigert, die NSA-Selektorenliste herauszugeben. Dagegen hat sich die G 10-Kommission an das Bundesverfassungsgericht gewandt. Der Antrag blieb jedoch erfolglos, da die G 10-Kommission nach Auffassung des Bundesverfassungsgerichts keine zulässige Antragstellerin darstellt und somit bereits die Zulässigkeit des Organstreits zu verneinen ist.¹⁵⁶

Während die G 10-Kommission bei der Vorabkontrolle immerhin die Möglichkeit hat, im Falle eines aus ihrer Sicht ungerechtfertigt erhobenen *Third Party Rule*-Einwands die Genehmigung der Maßnahme zu verweigern, kann sie sich gegen einen solchen Einwand nicht wehren, wenn der Nachrichtendienst bzw. die Aufsichtsbehörde ihn im Rahmen der Datenschutzkontrollen geltend macht.

Das führt zu der Frage, wieso die Einhaltung der *Third Party Rule* der Bundesregierung so wichtig ist (a.), warum das problematisch sein kann (b.) und ob der *Third Party Rule*-Einwand gegenüber unabhängigen Kontrolleuren tatsächlich geltend gemacht werden kann (c.).

a. *Begründung für die Notwendigkeit*

Obwohl die *Third Party Rule* den Empfänger rechtlich – auch völkerrechtlich¹⁵⁷ – nicht bindet¹⁵⁸, wird die Beachtung einer solchen Vereinbarung „als Selbstverständlichkeit vorausgesetzt“¹⁵⁹. Wenn der Empfänger der Informationen die Vertraulichkeitsver-

¹⁵² Vgl. [Teil 3 B. VIII. 2. c.](#); „Die Kontrolle durch die Kommission ist daher intensiver als jede gerichtliche Kontrolle sein könnte. Ihr gegenüber gibt es insbesondere weder eine Weigerung, irgendwelche Akten und Unterlagen vorzulegen (wie z.B. in § 99 VwGO), noch eine Dienstverschwiegenheit von Angehörigen des öffentlichen Dienstes.“, *Arndt*, G 10-Verfahren, 43, 57.

¹⁵³ Definition auf [Teil 2 A. III. 1. a. II\).](#)

¹⁵⁴ So eindeutig auch der Vorsitzende der G 10-Kommission des Bundes, Huber: „Eine umfassende Kontrolle nachrichtendienstlicher Tätigkeit des BND scheiterte bislang an der von dem Nachrichtendienst und auch der Bundesregierung behaupteten Pflicht zur Verschwiegenheit aufgrund der *Third Party Rule*.“, *Huber*, NVwZ-Beilage 2020, 3, 8.

¹⁵⁵ Auch bezüglich des Überwachungsprogramms „Eikonal“ ist die G 10-Kommission „vorsätzlich falsch informiert worden“, *Lachenmann*, DöV 2016, 501, 506 m. Verweis auf *Greis*, Operation Eikonal.

¹⁵⁶ BVerfG, Beschluss v. 20.9.2016 - 2 BvE 5/15.

¹⁵⁷ *Aust*, DöV 2020, 715, 721.

¹⁵⁸ Vgl. [Teil 2 A. III. 1. a. II\).](#)

¹⁵⁹ *Gazeas*, Übermittlung, S. 373.

einbarung bricht, riskiert er, zukünftige keine oder weniger sicherheitsrelevante Informationen zu erhalten.¹⁶⁰ Das gilt nicht nur gegenüber dem Absender der betroffenen Informationen, sondern kann die Wahrnehmung als vertrauenswürdiger Partner auch in den Augen anderer Kooperationspartner empfindlich schwächen.¹⁶¹ Da der Informationsfluss zwischen den Nachrichtendiensten von zentraler Bedeutung für die nachrichtendienstliche Arbeit ist¹⁶², wäre dann die Sicherheit der Bundesrepublik bedroht¹⁶³.

b. Missbrauchsgefahr

Die Third Party Rule kann innerstaatlich zum Problem werden, wenn andere Staatsgewalten, die nach der Vereinbarung unter Umständen als „Dritte“ gelten, ihrem verfassungsrechtlichen Auftrag der Regierungskontrolle nachkommen und ihr Kontrollbegehren mit Verweis auf eine solche Vereinbarung abgelehnt wird. In diesen Situationen kann der Kontrolleur nicht prüfen, ob es eine solche Vereinbarung tatsächlich gibt oder ob der Einwand lediglich vorgebracht wird, um ein unerwünschtes Kontrollbegehren ablehnen zu können. Daher birgt die Third Party Rule eine hohe Missbrauchsgefahr¹⁶⁴.

c. Unzulässig gegenüber unabhängigen Instanzen der Rechtskontrolle

Für die Frage, inwieweit die Third Party Rule einem Kontrollbegehren verfassungskonform entgegengehalten werden kann, kommt es entscheidend darauf an, wer kontrolliert. Es macht einen Unterschied, ob es um ein Gerichtsverfahren oder um das Infor-

¹⁶⁰ Vortrag der Bundesregierung in BVerfG, Beschluss v. 20.9.2016 - 2 BvE 5/15 - Rn. 26; Gärditz, DVBl 2015, 903, 904.

¹⁶¹ Gazeas, Übermittlung, S. 374.

¹⁶² Der Spiegel, „Ausländische Geheimdienste lieferten jeden zweiten Hinweis“ v. 6.2.2022, <https://www.spiegel.de/politik/deutschland/geplante-terroranschlaege-auslaendische-geheimdienste-lieferten-jeden-zweiten-hinweis-a-d0c347fb-f379-419b-b4bd-47b69c51c306> (abgerufen am 31.8.2024).

¹⁶³ Bund-Länder-Kommission Rechtsextremismus, Abschlussbericht v. 30.4.2013, Rn. 712, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/abschlussbericht-kommission-rechtsterrorismus-lang.pdf%3F__blob%3DpublicationFile%26v%3D2 (abgerufen am 31.8.2024); Gärditz, DVBl 2015, 903, 906.

¹⁶⁴ Führe zu einer „nicht unerheblichen Immunisierung der Sicherheitsbehörden gegen innerstaatliche Aufklärung“, es drohe eine „Flucht ins Internationale“, Gärditz, DVBl 2015, 903, 905, 908; „Arguably the greatest challenge to accountability in the area of international intelligence cooperation is the third party rule (...)“, „(...) the third party rule may be ‘over claimed’ in order to protect intelligence cooperation relationships“, Wills/Born, Intelligence cooperation, 277, 283 f.; Möllers, JZ 2017, 271, 277.

mationsgesuch eines Untersuchungsausschusses, ob es um Kontrollbegehren der Parlamentarischen Kontrollgremien oder unabhängiger Institutionen der Rechtskontrolle geht.¹⁶⁵

Jedenfalls gegenüber unabhängigen Institutionen der Rechtskontrolle kann der Third Party Rule-Einwand nicht erhoben werden. Das ergibt sich aus der Rechtsprechung des Bundesverfassungsgerichts, das klargestellt hat, dass die Kontrolle dadurch nicht behindert werden kann, weil die Einhaltung der Vereinbarung „durch eine strikt auf Geheimhaltung ausgerichtete Ausgestaltung der Kontrolle und durch Absprachen mit ausländischen Diensten gewährleistet werden kann“.¹⁶⁶ Das Gericht begründet dies neben der Geheimhaltungsverpflichtung auch damit, dass die unabhängigen Instanzen nicht „in das Parlament und dessen politische Kommunikationszusammenhänge eingebunden sind“.¹⁶⁷ Das gilt jedenfalls für alle Third Party Rule-Einwände, die auf Vereinbarungen beruhen, die nach der Entscheidung zur strategischen Ausland-Fernmeldeaufklärung getroffen wurden.¹⁶⁸ Gegenüber anderen Staaten sind diese Kontrolleure „dem informierten Dienst zuzurechnen“ und können daher keine „Dritten“ sein.¹⁶⁹

C. Rechtskontrolle des Unabhängigen Kontrollrats

Seit 2022 existiert ein neues Gremium zur Rechtskontrolle des BND, der UKRat.¹⁷⁰ Der UKRat ist in zwei Organe gegliedert, das gerichtsähnliche und das administrative Kontrollorgan (§ 40 Abs. 2 BNDG).

I. Kontrollmaßstab

Auch der UKRat ist ein Organ der Rechtskontrolle.

¹⁶⁵ Das ergibt sich u.a. aus einem Vergleich folgender Entscheidungen BVerfG, Beschluss v. 20.9.2016 - 2 BvE 5/15; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17; vgl. die Differenzierungen bei Gärditz, DVBl 2015, 903, 906 ff.; Ader, Hdb. Sicherheits- und Staatsschutzrecht, 612, 660 Rn. 164; Huber, NVwZ-Beilage 2020, 3, 9.

¹⁶⁶ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 – Rn. 224, vgl. auch BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 294; anders aber Dietrich, der annimmt, das Gericht lasse „Ausnahmen vom ungehinderten Zugang zu Informationen“ zu, beispielsweise in Fällen konkreter Bedrohungen für Leib und Leben deutscher Bürger, Dietrich, GSZ 2020, 173, 182.

¹⁶⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 294; Aust, DöV 2020, 715, 721.

¹⁶⁸ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 294.

¹⁶⁹ Bezieht hier auch das PKGr mit ein, Gärditz, DVBl 2015, 903, 907.

¹⁷⁰ Bewarder/Flade, Überwacher.

II. Kontrollgegenstand

Seine Hauptaufgabe besteht darin, die Rechtmäßigkeit der „technischen Aufklärung“ des BND „und damit einhergehende Übermittlungen und Kooperationen“ zu kontrollieren (§ 40 Abs. 1 BNDG). Vom Begriff der technischen Aufklärung erfasst sind die strategische Ausland-Fernmeldeüberwachung und Eingriffe in informationstechnische Systeme von Ausländern im Ausland.

1. Gerichtsähnliches Kontrollorgan

Der Kontrollgegenstand des gerichtsähnlichen Kontrollorgans (GeKon) wird in einem Zuständigkeitskatalog detailliert aufgezählt. So soll für die „wesentlichen Verfahrensschritte der technischen Aufklärung“ eine gerichtsähnliche Rechtskontrolle sichergestellt werden.¹⁷¹ Das GeKon ist sowohl für die Vorabkontrolle (a)) als auch für nachträgliche Kontrollen (b)) zuständig.¹⁷²

a. Vorabkontrolle des GeKon

Grundsätzlich prüft das GeKon die Rechtmäßigkeit der Maßnahmen vor ihrem Vollzug, das bedeutet, die Maßnahmen dürfen erst nach Bestätigung der Rechtmäßigkeit durch das GeKon umgesetzt werden.¹⁷³

Bei Gefahr im Verzug, wenn „andernfalls der Aufklärungszweck (...) vereitelt oder wesentlich erschwert würde“, findet davon abweichend eine vorläufige Vorabkontrolle durch ein Mitglied des GeKons statt (§ 23 Abs. 4 S. 3 BNDG ähnliche Formulierungen in § 11d Abs. 3 S. 1, § 23 Abs. 7 S. 2, § 37 Abs. 4 S. 3 BNDG¹⁷⁴). Gefahr im Verzug liegt vor, wenn Entscheidungen „nicht zügig“, sondern „sofort“ erfolgen müssen.¹⁷⁵ Auch bei Gefahr in Verzug kann die Maßnahme nur vollzogen werden, wenn die Anordnung bestätigt wird (§ 23 Abs. 4 S. 4 BNDG). In diesen Fällen muss die Prüfung durch den UKRat jedoch „unverzüglich“ nachgeholt werden. Als Beispiel für einen solchen Eilfall nennt der Gesetzgeber Entführungsfälle im Ausland, bei denen Daten erhoben werden

¹⁷¹ Dt. Bundestag, Drs. 19/26103, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 103.

¹⁷² Dt. Bundestag, Drs. 19/26103, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 103 ff, 106; *Graulich*, GSZ 2021, 121, 128.

¹⁷³ *Schmidt-Räntsch*, K&R 2022, 34, 35.

¹⁷⁴ Dass ein solches Eilverfahren für die Prüfung des qualifizierten Aufklärungsbedarfs gem. § 42 Abs. 1 Nr. 4, § 33 Abs. 2 BNDG nicht vorgesehen sei, sei ein Regelungsfehler. Im Wege des Analogieschlusses ist das GeKon auch dafür zuständig, *Schmidt-Räntsch*, K&R 2022, 34, 40.

¹⁷⁵ *Schmidt-Räntsch*, K&R 2022, 34, 40.

müssen, um unverzüglich Informationen „über neue krisenhafte Entwicklungen zur Verfügung stellen zu können.“¹⁷⁶ Weil damit selbst für den Eilfall eine vorläufige, unabhängige Vorabkontrolle sichergestellt ist, ist die Norm konventionskonform ausgestaltet.

§ 42 BNDG legt fest, welche Maßnahmen des BND genehmigungspflichtig sind.

aa) Strategische Ausland- Fernmeldeüberwachung gem. § 19 BNDG

Zunächst ist das GeKon für die Genehmigung von Maßnahmen im Rahmen der strategischen Ausland-Fernmeldeüberwachung gem. § 42 Abs. 1 Nr. 1, § 23 Abs. 4, § 19 BNDG zuständig.

Damit steht dessen Kontrolle „am Anfang jedweder Tätigkeit des BND im Rahmen der strategischen Ausland-Fernmeldeaufklärung und spannt so einen Schirm auf über alle aus ihr abgeleiteten Datenerhebungen“.¹⁷⁷

(1) Reichweite der Kontrolle

Was das GeKon inhaltlich kontrollieren kann, wird zunächst durch die Anordnung bestimmt, die der BND ihm zur Genehmigung vorlegt. Was der BND in der Anordnung zwingend angeben muss, wird in § 23 Abs. 2 und Abs. 3 BNDG detailliert. Demnach ist in der Anordnung zunächst „der Aufklärungszweck“ zu nennen, der sich nach § 19 Abs. 1 BNDG richtet. Aus dieser Norm ergibt sich, dass Maßnahmen entweder zum Zweck der politischen Unterrichtung der Bundesregierung (§ 19 Abs. 1 Nr. 1) oder zur Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung (§ 19 Abs. 1 Nr. 2) angeordnet werden können.

Außerdem muss das „Aufklärungsthema“ gem. § 19 Abs. 3 oder § 19 Abs. 4 BNDG genannt werden.¹⁷⁸ Maßnahmen zur politischen Unterrichtung der Bundesregierung (§ 19 Abs. 1 Nr. 1 BNDG) sind demnach nur zulässig, wenn sie von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind und das Bundeskanzleramt den BND damit beauftragt hat (§ 19 Abs. 3). Wenn die Maßnahme zur Früherkennung von aus dem Ausland drohenden Gefahren angeordnet wurde (§ 19 Abs. 1 Nr. 2 BNDG), sind die Anforderungen an den Gefahrenbereich etwas höher: hier muss nicht nur die außen- und sicherheitspolitische Bedeutung bejaht werden und

¹⁷⁶ Dt. Bundestag, Drs. 19/26103, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 103.

¹⁷⁷ Dt. Bundestag, Drs. 19/26103, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 103.

¹⁷⁸ Erläuterung bei Steiner, GSZ 2023, 124, 127.

eine Beauftragung des Bundeskanzleramts vorliegen, sondern es müssen zusätzlich tatsächliche Anhaltspunkte dafür gegeben sein, dass Erkenntnisse zu bestimmten Gefahrenbereichen (§ 19 Abs. 4 Nr. 1) oder zum Schutz bestimmter Rechtsgüter (§ 19 Abs. 4 Nr. 2) gewonnen werden können. Außerdem ist die Art der Gefahr zu detaillieren (§ 23 Abs. 3 BNDG).

Darüber hinaus sind der „geografische Fokus“ und die „Dauer“ der Maßnahme zu nennen (§ 23 Abs. 2 Nr. 3, 4 BNDG). Zusätzlich muss die Notwendigkeit der Maßnahme begründet werden (§ 23 Abs. 2 Nr. 5 BNDG). Mit diesen Angaben werde der vom BND mit der Anordnung verfolgte Erhebungszweck näher beschrieben, erläutert Steiner (ehemaliges Mitglied des GeKon).¹⁷⁹ Wie detailliert die Begründung sein muss, ist allerdings weder im Gesetz noch in den Gesetzgebungsmaterialien festgelegt.

Obwohl es rechtliche Vorgaben für die Anordnung gibt, fällt vor allem auf, was nicht vorgeschrieben ist: der BND muss in der Anordnung für eine Maßnahme der strategischen Ausland-Fernmeldeaufklärung nicht angeben, anhand welcher Suchbegriffe er den Telekommunikationsverkehr analysiert.¹⁸⁰ Den Vorschlag von Graulich, § 23 BNDG wegen der „Erfahrungen“ aus dem NSA-Untersuchungsausschuss und der „Entstehungsgeschichte des Gesetzes“ so auszulegen, dass die Selektoren dem UKRat vorzulegen sind¹⁸¹, wurde in der Praxis offenbar nicht angenommen, denn das ehemalige Mitglied des GeKon Steiner schreibt, dass die Suchbegriffe in der Anordnung nicht genannt werden müssen, obwohl Graulich „augenscheinlich“ die Möglichkeit sehe, eine Nennung „zu verlangen“¹⁸².

(2) Verletzung von Konventionsrecht

Dass das Kontrolldesign des GeKon keine unabhängige Vorabkontrolle der Selektoren bzw. zumindest von Kategorien von Selektoren vorsieht, sondern lediglich eine ex post-Kontrolle durch das administrative Kontrollorgan etabliert, macht es konventionswidrig.¹⁸³

Nach der Rechtsprechung des EGMR müssen im Antrag zur Genehmigung „mindestens“ die Kategorien von Selektoren, die benutzt werden sollen, bezeichnet werden. Der EGMR verdeutlicht, dass er es wegen der enormen Bedeutung der Selektorenfestlegung vorziehen würde, wenn die Selektoren im Antrag konkret benannt würden und dass er die Bezeichnung von Kategorien anstatt konkreter Selektoren nur akzeptiert, um

¹⁷⁹ Steiner, GSZ 2023, 124, 127.

¹⁸⁰ Markard, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 7.

¹⁸¹ Graulich, GSZ 2021, 121, 124.

¹⁸² Steiner, GSZ 2023, 124, 128 m. Verweis auf Graulich, GSZ 2021, 121, 124.

¹⁸³ So auch Bäcker, Beschwerdeschrift BNDG II, S. 101; Wetzling, Bedingt kontrollfähig, S. 13; Steiner, GSZ 2024, 32, 36.

den praktischen Bedürfnissen mancher Konventionsstaaten entgegenzukommen.¹⁸⁴ Dass keine Vorabkontrolle der Selektoren vorgesehen ist, verwundert insbesondere, weil in den Anträgen an die G 10-Kommission alle Suchbegriffe genannt werden müssen.¹⁸⁵

Darüber hinaus verpflichtet § 23 Abs. 2 S. 2 BNDG nicht dazu, in der Anordnung die verwendeten Träger elektronischer Kommunikation und Kommunikationsrouten zu benennen, was die Norm konventionswidrig macht.¹⁸⁶

bb) Gezielte Erhebungen gem. §§ 20, 21 Abs. 2 BNDG

Für gezielte Erhebungen im Rahmen der strategischen Ausland-Fernmeldeaufklärung gelten gem. §§ 20, 21 Abs. 2 BNDG besondere Voraussetzungen. Ob diese Vorgaben eingehalten werden, prüft das GeKon gem. §§ 42 Abs. 1 Nr. 2, 23 Abs. 5, Abs. 7 BNDG ex ante.

(1) Reichweite der Kontrolle

Von dem Genehmigungsvorbehalt erfasst ist erstens die Erhebung von personenbezogenen Inhaltsdaten mit Hilfe von Suchbegriffen, die sich auf Einrichtungen der Europäischen Union, öffentliche Stellen ihrer Mitgliedstaaten oder Unionsbürger beziehen (§ 23 Abs. 5 S. 1 Nr. 1, § 20 Abs. 1, § 19 Abs. 5 BNDG). Zweitens geht es um gezielte Erhebungen personenbezogener Daten von möglichen Gefahrverursachern (§ 23 Abs. 5 S. 1 Nr. 2, § 20 Abs. 2 BNDG). Drittens ist auch die Anordnung zur gezielten Erhebung von Daten aus einer Vertraulichkeitsbeziehung genehmigungspflichtig (§ 23 Abs. 5 S. 1 Nr. 3, § 21 Abs. 2 BNDG). Keiner Vorabkontrolle unterliegen solche Daten, wenn dafür bereits eine Beschränkungsanordnung gem. §§ 3, 5, 8 G 10 vorliegt. Dann muss der UKRat darüber lediglich unterrichtet werden (§ 23 Abs. 5 S. 2, 3 BNDG).

Für Anordnungen zu gezielten Datenerhebungen gelten gem. § 23 Abs. 6 BNDG spezifische Voraussetzungen. Demnach muss in der Anordnung die strategische Aufklärungsmaßnahme benannt werden, in deren Rahmen die gezielte Datenerhebung erfolgt (§ 23 Abs. 6 S. 1 Nr. 1 BNDG). Zudem sind das Ziel und die Dauer der Maßnahme anzugeben (§ 23 Abs. 6 S. 1 Nr. 2, 3 BNDG). Die Anordnung muss begründet werden (§ 23 Abs. 6 S. 1 Nr. 4 BNDG). Die einzelnen Suchbegriffe, die zur gezielten Datenerhebung verwendet werden, müssen jedoch ausdrücklich nicht benannt werden (§ 23 Abs. 6 S. 2 BNDG).

¹⁸⁴ EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 353 – Big Brother Watch gg. UK; EGMR 25.5.2021-35252/08 Rn. 266 ff. – Centrum för Rättvisa gg. Schweden; vgl. [Teil 2 B. I. 4. b. dd.](#)

¹⁸⁵ Vgl. [Teil 3 B. II. 1. a.](#)

¹⁸⁶ Vgl. [Teil 2 B. I. 4. b. dd.](#); Steiner, GSZ 2024, 32, 36.

(2) Verfassungswidrige Ausklammerung der Kontrolle von Suchbegriffen

Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine unabhängige Vorabkontrolle von Suchbegriffen verfassungsrechtlich zwingend, wenn die Suchbegriffe auf mögliche Gefahrverursacher oder Vertraulichkeitsbeziehungen abzielen.¹⁸⁷ Weil die Suchbegriffe für die gezielte Datenerhebung in der Anordnung nicht genannt werden müssen (§ 23 Abs. 6 S. 2 BNDG), kann das GeKon, das die Anordnung genehmigt, die Suchbegriffe nicht kontrollieren.¹⁸⁸

Die Kontrolle von Suchbegriffen durch das AdKon kann dieses Defizit nicht ausgleichen, weil es sich dabei um eine laufende bzw. nachträgliche Kontrolle handelt. Im Ergebnis ist § 23 Abs. 6 S. 2 BNDG mit den Vorgaben des Bundesverfassungsgerichts deshalb nicht vereinbar und verfassungswidrig.¹⁸⁹

(3) Verfassungswidrige Ausnahme von der Vorabkontrolle

Grundsätzlich unterliegen Anordnungen zu gezielten Überwachungen in verfassungskonformer Weise dem Genehmigungsvorbehalt zugunsten des GeKon (§ 23 Abs. 7 S. 1, Abs. 6 BNDG). Dies gilt nicht, wenn keine Anordnung erfolgen muss, weil bereits eine Beschränkungsanordnung der G 10-Kommission nach §§ 3, 5 oder § 8 G 10 vorliegt (§ 23 Abs. 5 S. 2 BNDG). Dann muss das GeKon nur unterrichtet werden (§ 23 Abs. 5 S. 3 BNDG). Die Kontrolle durch die G 10-Kommission erfüllt die Vorgaben des Bundesverfassungsgerichts zum gerichtsähnlichen Kontrollorgan jedoch derzeit nicht, weil die G 10-Kommission unter anderem nicht mit einer „maßgeblichen Zahl“ an Richtern besetzt ist¹⁹⁰ und ihre Mitglieder nur ehrenamtlich tätig sind. Mithin ist die Beschränkung der Zuständigkeit des GeKon zugunsten der G 10-Kommission verfassungswidrig.¹⁹¹

cc) Feststellung des „qualifizierten Aufklärungsbedarfs“ bei Kooperationen

Wenn der BND im Rahmen einer Kooperation mit einem ausländischen Nachrichtendienst unselektierte, personenbezogene Verkehrsdaten weiterleiten möchte, muss dafür gem. § 33 Abs. 2 BNDG ein „qualifizierter Aufklärungsbedarf“ vorliegen. Dass die Voraussetzungen von § 33 Abs. 2 BNDG erfüllt sind, muss zunächst vom GeKon geprüft und bestätigt werden (§ 42 Abs. 1 Nr. 3 BNDG).

¹⁸⁷ Vgl. [Teil 2 A. III. 2. b. ii\).](#)

¹⁸⁸ Bäcker, Beschwerdeschrift BNDG II, S. 101; Steiner, GSZ 2023, 124, 128.

¹⁸⁹ Bäcker, Beschwerdeschrift BNDG II, S. 102 f.

¹⁹⁰ Vgl. [Teil 2 A. III. 2. b. ii\).](#)

¹⁹¹ Bäcker, Beschwerdeschrift BNDG II, S. 99 f.

dd) Möglicher Kernbereichsbezug von Daten aus der strategischen Ausland-Fernmeldeaufklärung und der Online-Durchsuchung von Ausländern im Ausland

Das GeKon übernimmt zudem die Rolle der unabhängigen Stelle¹⁹², soweit bei der Weiterverarbeitung von Daten aus der strategischen Ausland-Fernmeldeaufklärung Zweifel bestehen, ob Daten, die nicht unverzüglich gelöscht werden sollen, dem Kernbereich privater Lebensgestaltung zuzuordnen sind (§ 42 Abs. 1 Nr. 4, § 22 Abs. 3 BNDG). Es ist auch zuständig für die entsprechende Prüfung bei Daten aus der Online-Durchsuchung von Ausländern im Ausland (§ 36 Abs. 3 BNDG).¹⁹³

ee) Eingriffe in informationstechnische Systeme gem. § 34 BNDG

Wenn der BND Eingriffe in informationstechnische Systeme von Ausländern im Ausland gem. § 34 BNDG anordnet oder einen solchen Eingriff verlängern möchte, muss das GeKon dies vorab genehmigen (§ 42 Abs. 3 Nr. 1, § 37 Abs. 1, 4 BNDG).

Das ehemalige Mitglied des GeKon, Steiner, hat darauf hingewiesen, dass die Prüfung des Tatbestands von § 34 Abs. 1 Nr. 2, Abs. 3 BNDG problematisch ist: Welche Informationen von *herausgehobener* außen- und sicherheitspolitischer Bedeutung und nicht nur von einfacher außen- und sicherheitspolitischer Bedeutung gem. § 1 Abs. 2, § 19 Abs. 2 BNDG sind, sei eine politische Frage. Deshalb solle die Bundesregierung diese Wertung im Rahmen ihres die Aufklärungstätigkeit des BND anleitenden Auftragsprofils vornehmen, statt dies dem BND und dem GeKon zu überlassen¹⁹⁴. Der Gesetzgeber muss solche Anregungen der Kontrolleure unbedingt berücksichtigen, weil die Ausgestaltung der Verhaltensnormen entscheidend für die Qualität der Rechtskontrolle ist¹⁹⁵.

Das GeKon kontrolliert im Rahmen von § 34 BNDG „nicht notwendigerweise eine gezielt gegen einen individuellen Grundrechtsträger oder dessen IT-Systeme gerichtete Datenerhebungsmaßnahme“, sondern entscheidet, ob ein Eingriff in informationstechnische Systeme vorgenommen werden kann, um ein „nachrichtendienstlich relevante[s] Them[a] bei nachrichtendienstlich relevanten Akteuren“ aufzuklären.¹⁹⁶

§ 37 Abs. 2 BNDG regelt die notwendigen Bestandteile einer Anordnung für einen Eingriff in informationstechnische Systeme von Ausländern im Ausland. Demnach

¹⁹² Vgl. [Teil 2 A. III. 2. b.](#)

¹⁹³ Offensichtlich hat man vergessen, dies im Katalog von § 42 BNDG aufzunehmen.

¹⁹⁴ Welche Informationen von *herausgehobener* außen- und sicherheitspolitischer Bedeutung und nicht nur von einfacher außen- und sicherheitspolitischer Bedeutung gem. § 1 Abs. 2, § 19 Abs. 2 BNDG sind, sei eine politische Frage. Deshalb solle die Bundesregierung diese Wertung im Rahmen ihres die Aufklärungstätigkeit des BND anleitenden Auftragsprofils vornehmen, statt dies dem BND und dem GeKon zu überlassen, *Steiner*, GSZ 2023, 124, 130.

¹⁹⁵ Vgl. [Teil 1 B. III. 4.](#)

¹⁹⁶ *Steiner*, GSZ 2023, 124, 129.

sind in der schriftlichen Anordnung der Aufklärungszweck (Nr. 1) und das verfolgte Aufklärungsthema (Nr. 2) anzugeben. Zudem ist in der Anordnung das Ziel (Nr. 3) festzulegen, das bedeutet sie muss Angaben zur „Zielperson“, zum „Zielsystem“ oder dem „Zielbereich“ der Datenerhebung enthalten.¹⁹⁷

Darüber hinaus müssen „Art, Umfang und Dauer der individuellen Aufklärungsmaßnahme“ (Nr. 4) beschrieben werden. Weil die Anordnung und somit auch die Prüfung des GeKon sich in der Regel nicht auf eine einzelne Maßnahme beziehen, bedeutet die Angabe von „Art“ und „Umfang“ nicht, dass in der Anordnung „die technische Herangehensweise“ oder der „konkret[e] Umfang der Datenerhebung“ dargestellt werden.¹⁹⁸

Auch die „Dauer“ gem. § 37 Abs. 2 Nr. 4 BNDG bezieht sich nicht auf eine konkrete Datenerhebung aus einem informationstechnischen System. Gemeint ist damit lediglich, dass der BND angeben muss, wie lange die Anordnung gültig ist.¹⁹⁹

Außerdem muss der Antrag begründet werden (Nr. 5). Darüber hinaus ist die „Festlegung eines längeren Prüfzeitraums nach § 34 Abs. 7 S. 2 oder Abs. 9“ anzugeben. Dabei geht es darum, dass der BND grundsätzlich unverzüglich prüfen muss, ob die erhobenen Daten für die politische Unterrichtung der Bundesregierung oder zur Früherkennung von aus dem Ausland drohenden Gefahren erforderlich ist (§ 34 Abs. 7 S. 1 BNDG). Falls eine unverzügliche Prüfung nicht möglich ist, kann der BND abweichend davon einen Prüfungszeitraum von drei Jahren festlegen, wenn der UKRat dem zustimmt (§ 34 Abs. 7 S. 2 BNDG). Die Norm ist auch anwendbar, soweit es um die Ausweitung eines informationstechnischen Systems geht, das sich im Besitz des BND befindet (§ 34 Abs. 9 BNDG).

ff) Übermittlung von Daten aus Vertraulichkeitsbeziehungen

Übermittelt der BND Daten, die aus einer Vertraulichkeitsbeziehung stammen, an inländische öffentliche Stellen und andere inländische Stellen sowie an ausländische öffentliche oder über- und zwischenstaatliche Stellen, benötigt er dafür eine Genehmigung des GeKon. Das gilt zunächst für Daten, die er aus einer Maßnahme der strategischen Ausland-Fernmeldeaufklärung gewonnen hat (§ 42 Abs. 1 Nr. 5, § 11d i. V. m. § 11g BNDG). Vertraulichkeitsbeziehungen sind gem. § 21 Abs. 1 S. 2 BNDG „solche von Geistlichen, Verteidigern, Rechtsanwälten und Journalisten, die dem Schutz des § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 und 5 sowie Satz 2 der Strafprozessordnung unterfallen würden“.

¹⁹⁷ Steiner, GSZ 2023, 124, 129.

¹⁹⁸ Steiner, GSZ 2023, 124, 129.

¹⁹⁹ Steiner, GSZ 2023, 124, 129.

Bis zum 1. Januar 2024 war das GeKon außerdem für die Genehmigung einer Übermittlung von Daten mit Vertraulichkeitsbezug aus einem Eingriff in informationstechnische Systeme gem. § 34 BNDG zuständig (§§ 43 Abs. 3 Nr. 2, 38 Abs. 8 und 39 Abs. 6 a.F. BNDG). Bei der Reform der Übermittlungsvorschriften des BNDG im November 2023 sind die §§ 38, 39 BNDG, auf die § 42 Abs. 3 Nr. 2 BNDG verweist, jedoch gestrichen worden.²⁰⁰ Dabei kann es sich nur um einen Gesetzgebungsfehler handeln, denn es gibt keinen Grund, wieso der UKRat für die Genehmigung einer Übermittlung solcher Daten, die aus der strategischen Ausland-Fernmeldeaufklärung gewonnen wurden, zuständig sein soll, für solche aus Maßnahmen gem. § 34 BNDG hingegen nicht. Dass es sich um einen Fehler handeln muss, beweist der dem widersprechende § 11d Abs. 2, 3 BNDG: Demnach ist der UKRat für die Genehmigung dieser Übermittlungen ausdrücklich zuständig. Das GeKon ist daher im Ergebnis weiterhin für die Genehmigung zuständig. Der Gesetzgeber sollte die Verweise in § 42 Abs. 3 Nr. 2 BNDG aktualisieren.

b. Sonstige Rechtmäßigkeitskontrolle „nach dem Vollzug“

Darüber hinaus ergibt sich aus dem Zuständigkeitskatalog, dass das GeKon bestimmte Maßnahmen und Gegenstände nach dem Vollzug auf ihre Rechtmäßigkeit hin überprüft. Die entsprechenden Sachverhalte müssen dem GeKon „unverzüglich“ vorgelegt werden (§ 42 Abs. 5 BNDG).²⁰¹

Dies betrifft zunächst die Verwendung von Daten, bei denen sich erst im Rahmen der Verarbeitung zeigt, dass sie aus einer Vertraulichkeitsbeziehung stammen (§ 42 Abs. 2 Nr. 1, § 23 Abs. 3 BNDG; § 42 Abs. 4 Nr. 1, § 35 Abs. 3 BNDG). Zudem kontrolliert das GeKon Dienstvorschriften des BND zur technischen und organisatorischen Umsetzung der technischen Aufklärung, „soweit diese Regelungen zur Datenauswertung“ enthalten (§ 42 Abs. 2 Nr. 3, § 62 BNDG). Außerdem prüft es Sachverhalte, in denen das AdKon gegenüber dem BND eine Beanstandung ausgesprochen hat, der nicht abgeholfen wurde und in denen das AdKon das GeKon um eine abschließende Entscheidung ersucht (§ 42 Abs. 2 Nr. 4, § 42 Abs. 4 Nr. 3, § 52 Abs. 3 BNDG).

Schließlich kontrolliert das GeKon die Zweckänderung von Daten, die aus der strategischen Ausland-Fernmeldeaufklärung gewonnen und ursprünglich zur politischen Unterrichtung verwendet wurden und dann zur Verhinderung einer unmittelbar be-

²⁰⁰ Dt. Bundestag, Drs. 20/8627, Entwurf der Bundesregierung zur Änderung des BNDG v. 2.10.2023, S. 22; BGBl I Nr. 410 v. 29.12.2023, S. 12.

²⁰¹ Dt. Bundestag, Drs. 19/26103, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 104.

vorstehenden Gefahr für besonders wichtige Rechtsgüter an inländische oder an ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie an andere ausländische Stellen²⁰² übermittelt werden sollen.

Bis zum 1. Januar 2024 war das GeKon außerdem für die Kontrolle der Zweckänderung von Daten zuständig, die durch Eingriffe in informationstechnische Systeme gewonnen wurden und die ursprünglich zur politischen Unterrichtung verwendet wurden und dann zur Verhinderung einer unmittelbar bevorstehenden Gefahr für besonders wichtige Rechtsgüter an inländische und ausländische Stellen übermittelt werden sollten²⁰³. Bei der Reform der Übermittlungsvorschriften des BNDG im November 2023 sind die §§ 38, 39 BNDG, auf die § 42 Abs. 4 Nr. 2 BNDG verweist, jedoch gestrichen worden.²⁰⁴ Anders als bei der Übermittlung von Daten aus Vertraulichkeitsbeziehungen enthalten die neuen Übermittlungsnormen jedoch keinen Genehmigungsvorbehalt zugunsten des UKRats.²⁰⁵ Denkbar wäre, die Zuständigkeit über den Verweis in § 42 Abs. 2 Nr. 2 BNDG herzuleiten, weil die Übermittlungsnormen, auf die er verweist, sich auch auf Daten gem. § 34 BNDG beziehen. Dagegen spricht jedoch, dass § 42 Abs. 2 BNDG ausdrücklich auf die Kontrolle der Rechtmäßigkeit im Rahmen der strategischen Ausland-Fernmeldeaufklärung bezogen ist.

Im Ergebnis ist das GeKon für die laufende Kontrolle solcher Zweckänderungen von Daten aus Eingriffen in informationstechnische Systeme gem. § 34 BNDG nicht mehr zuständig. Dabei kann es sich nur um einen Fehler handeln, der behoben werden muss. Falls keine Richtigstellung in diesem Sinne erfolgt, stellt sich die Frage, wieso die Zweckänderung bei Daten aus der strategischen Ausland-Fernmeldeaufklärung kontrolliert werden soll, bei Daten aus Eingriffen in informationstechnische Systeme gem. § 34 BNDG hingegen nicht. Das Problem könnte gelöst werden, indem man festlegt, dass § 42 Abs. 4 Nr. 2 entsprechend dem § 42 Abs. 2 Nr. 2 auf die §§ 11b Abs. 5, § 11c Abs. 3, § 11e Abs. 4 und § 11f Abs. 3 BNDG verweist.

2. Administratives Kontrollorgan

Die Zuständigkeit des Administrativen Kontrollorgans (AdKon) richtet sich nach § 51 BNDG.

²⁰² § 42 Abs. 2 Nr. 2, § 11b Abs. 5, § 11c Abs. 3 BNDG; § 42 Abs. 2 Nr. 2, § 11e Abs. 4, § 11f Abs. 3 BNDG.

²⁰³ § 42 Abs. 4 Nr. 2, § 38 Abs. 7 BNDG a.F.; § 42 Abs. 4 Nr. 2, § 39 Abs. 4 BNDG a.F.

²⁰⁴ Dt. Bundestag, Drs. 20/8627, Entwurf der Bundesregierung zur Änderung des BNDG v. 2.10.2023, S. 22; BGBl I Nr. 410 v. 29.12.2023, S. 12.

²⁰⁵ Vgl. [Teil 3 C. II. 1. a. ff.](#)

a. Zuständigkeit

Das AdKon unterstützt das GeKon bei der Durchführung seiner Kontrollbefugnisse²⁰⁶ und ist für die nachträgliche²⁰⁷ Rechtskontrolle derjenigen Bereiche der technischen Aufklärung durch den BND zuständig, die nicht der Rechtskontrolle durch das GeKon unterliegen, wobei es „insbesondere“ die Rechtmäßigkeit von Suchbegriffen kontrollieren kann, soweit nicht die „originäre Zuständigkeit“ des GeKons eröffnet ist (§ 51 Abs. 1 BNDG). Das GeKon bestimmt die „konkrete Ausgestaltung der Prüftätigkeit“ des AdKon in regelmäßigen Abständen und kann konkrete, einzelfallbezogene Prüfungsaufträge erteilen (§ 52 Abs. 3 BNDG). Innerhalb des durch das GeKon vorgegebenen Rahmens kann das AdKon „eigeninitiativ prüfungsrelevante Aspekte aufgreifen, die ihm bei der Kontrolle aufgefallen sind“.²⁰⁸

Eine Aufgabe des AdKon besteht darin, zu prüfen, ob der BND die vom GeKon bestätigten Anordnungen rechtmäßig umsetzt.²⁰⁹ Daneben kontrolliert es beispielsweise die Eignungsprüfung gem. § 24 BNDG, wonach der BND personenbezogene Daten aus Telekommunikationsnetzen nur erheben und auswerten darf, soweit dies zur Bestimmung geeigneter Telekommunikationsnetze (Alt. 1) oder geeigneter Suchbegriffe (Alt. 2) erforderlich ist.²¹⁰ Von seinem Prüfungsauftrag erfasst ist unter anderem auch die Einhaltung von Löschfristen, der Übermittlungs- und Kooperationsnormen (§ 29 ff. BNDG), der Pflichten zur Benachrichtigung Betroffener (§ 59 BNDG) und die Kontrolle solcher Dienstvorschriften, die nicht auf die Auswertung bezogen sind (§ 62 BNDG).²¹¹ Das Mitglied des GeKon, Johanna Schmidt-Räntsch, nennt als weitere Aufgabe unter anderem die Prüfung, ob Datenerhebungen entgegen der Vorgabe zu Zwecken der Wirtschaftsspionage erfolgen (§ 19 Abs. 9 BNDG).²¹²

Die Kontrolle des AdKon kann sich letztlich auf die Einhaltung aller rechtlichen Bestimmungen beziehen, die für die technische Aufklärung des BND gelten.

²⁰⁶ Das gerichtsähnliche Kontrollorgan könne beispielsweise auf dessen Expertise zugreifen, um seine Entscheidungen vorzubereiten, Dt. Bundestag, Drs. 19/26103, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 111.

²⁰⁷ Dt. Bundestag, Drs. 19/26103, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 104.

²⁰⁸ *Hoch/Schmidt/Räntsch/Brunst*, NVwZ 2023, 712, 713.

²⁰⁹ *Schmidt-Räntsch*, K&R 2022, 34, 37.

²¹⁰ Wegen der zentralen Bedeutung von § 24 BNDG für den BND forderte Wetzling, dessen Kontrolle in § 52 Abs. 1 explizit aufzuzählen oder eine Vorabkontrolle zu etablieren, *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 9.

²¹¹ *Löffelmann/Zöller*, Nachrichtendienstrecht, S. 263.

²¹² *Schmidt-Räntsch*, K&R 2022, 34, 36.

b. Notwendigkeit eines Positivkatalogs?

Vereinzelt wurde im Rahmen des Gesetzgebungsverfahrens gefordert, dass auch für die Tätigkeiten des administrativen Kontrollorgans ein dem § 42 BNDG vergleichbarer Positivkatalog der Zuständigkeiten normiert werden solle, „da andernfalls Streitigkeiten mit dem BND über seine Kompetenzen absehbar“ seien.²¹³ Dem ist insoweit zuzustimmen, als § 51 Abs. 1 BNDG nicht so deutlich formuliert ist, wie das Bundesverfassungsgericht es im Urteil zur strategischen Auslands-Fernmeldeaufklärung entschieden hat: das administrative Kontrollorgan soll den „gesamten Prozess der strategischen Überwachung“ auf seine Rechtmäßigkeit hin überprüfen.“²¹⁴ Aus der Gesetzesbegründung ergibt sich, dass die beiden Gremien des UKRats den gesamten Prozess der technischen Aufklärung im Zusammenspiel kontrollieren, jedoch nicht, dass dies auch für das AdKon an sich gilt.²¹⁵ Darin liegt jedoch kein Widerspruch zu den Vorgaben der Rechtsprechung: Weil der Gesetzgeber dem richterähnlichen Kontrollgremium nicht nur die Vorabkontrolle, sondern auch die ex-post Kontrolle mancher Maßnahmen übertragen hat und die nachträgliche Rechtskontrolle daher von beiden Gremien übernommen wird, kommt es entscheidend darauf an, dass im Ergebnis der „gesamte Prozess der strategischen Überwachung“ auf seine Rechtmäßigkeit hin geprüft wird. Dem wird die Regelung gerecht. Ein Positivkatalog ist nicht notwendig, weil sich aus dem Gesetzesentwurf ergibt, dass das AdKon für die ex-post Kontrolle der gesamten strategischen Aufklärung zuständig sein soll, soweit keine Zuständigkeit des GeKon gem. § 42 Abs. 2 bzw. 4 BNDG gegeben ist. Nichtsdestotrotz wäre es zur Klarstellung sinnvoll gewesen, das AdKon zur Rechtskontrolle „aller“ (statt „der“) Bereiche zu ermächtigen, die nicht der Kontrolle durch das GeKon unterliegen (§ 51 Abs. 1 BNDG).

c. Verfassungswidrigkeit wegen fehlender Protokollierungspflicht

Kontrolle setzt voraus, dass der Kontrolleur Kenntnis über den Kontrollgegenstand hat. In diesem Zusammenhang betont das Bundesverfassungsgericht, dass die verschiedenen Schritte der Datenverarbeitung in einer Weise protokolliert werden müssen, die

²¹³ Markard, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 10; kritisch auch Wetzling, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 6 ff.

²¹⁴ Dazu gehören „sowohl Einzelentscheidungen und Verfahrensabläufe als auch die Gestaltung der Datenverarbeitung und der Filterprozesse sowie der hierfür verwendeten technischen Hilfsmittel, BVerfG, Urteil v. 19.5.2020, 1 BvR 2835/17 Rn. 276.

²¹⁵ Dr. Bundestag, Drs. 19/26103, Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 111.

eine wirksame Kontrolle ermöglicht.²¹⁶ Auch der EGMR forderte detaillierte Aufzeichnungen auf allen vier Stufen der „bulk interception“, wobei die Filterung der Daten anhand der Selektoren die zweite Stufe darstellt.²¹⁷

Das BNDG verpflichtet den BND hingegen nicht, die verwendeten Selektoren zu protokollieren. Die in § 51 Abs. 1 S. 2 BNDG normierte Kontrolle von Suchbegriffen durch das AdKon ist damit praktisch nicht umsetzbar.²¹⁸ Insoweit ist das Gesetz sowohl verfassungs- als auch konventionswidrig.

Zusätzlich verpflichtet das BNDG in verfassungs- und konventionswidriger Weise nicht zur Protokollierung der einzelnen Datenverarbeitungsschritte. Soweit Löschungen für „Kontrollen der Datenverarbeitung“ protokolliert werden sollen, ist damit die interne Datenschutzkontrolle durch den BND gemeint.²¹⁹ Diese Protokolle unterstützen die externen Kontrollorgane nicht.

III. Zeitpunkt

Das GeKon prüft sowohl ex ante (§ 42 Abs. 1, 3 BNDG) als auch „nach dem Vollzug“ (§ 42 Abs. 2, 4 BNDG). Das AdKon kontrolliert laufend bzw. nachträglich.²²⁰

IV. Kontrolleur

Der UKRat, eine oberste Bundesbehörde gem. § 41 Abs. 1 BNDG, setzt sich aus dem gerichtsähnlichen und dem administrativen Kontrollorgan zusammen. Somit ist er organisatorisch Teil der Exekutive, nimmt funktional jedoch Aufgaben der Judikative wahr.²²¹ Der Gesetzgeber hat sich in verfassungskonformer Weise dazu entscheiden, die gerichtsähnliche und die administrative Kontrolle „zu zwei schlichten Kontrollfunktionen“ unter dem „einheitlichen institutionellen Dach des Unabhängigen Kontrollrats“ auszuformen, obwohl er nach den Vorgaben des Urteils zur strategischen Ausland-Fernmeldeaufklärung auch die Möglichkeit gehabt hätte, beides organisatorisch zu trennen.²²²

²¹⁶ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 291.

²¹⁷ Vgl. [Teil 2 B. I. 4. b. ee](#)), EGMR 25.5.2021 – 58170/13, 62322/14, 24960/15 Rn. 356, 499 – Big Brother Watch gg. UK; EGMR 25.5.2021 -35252/08 Rn. 270 – Centrum för Rättvisa gg. Schweden.

²¹⁸ *Bäcker*, Beschwerdeschrift BNDG II 2022, S. 102.

²¹⁹ *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 4, der deshalb vorschlägt „überall dort, wo im BND-GE mit Blick auf Protokollaten die interne Kontrolle des BND angesprochen wird, einen Einschub“ zu ergänzen, sodass „die Protokollaten auch den Kontrollorganen des UKRat uneingeschränkt zugänglich zu machen sind“.

²²⁰ Dt. Bundestag, Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 104.

²²¹ *Barczak*, KritV 2021, 91, 128, vgl. [Teil 1 A. I. 1. b.](#)

²²² *Barczak*, KritV 2021, 91, 127.

1. *Gerichtsähnliches Kontrollorgan*

Zur Ausgestaltung des GeKons enthält das BNDG detaillierte Vorgaben.

a. Anzahl der Mitglieder, Ernennung, Amtszeit und Organisation

Ihm gehören sechs Mitglieder an, die vom Parlamentarischen Kontrollgremium mit einfacher Mehrheit für eine einmalige Amtszeit von zwölf Jahren²²³ gewählt werden (§ 43 Abs. 1, 4, § 45 Abs. 2 BNDG). Ihre Amtszeit endet grundsätzlich nach zwölf Jahren oder mit Vollendung des 70. Lebensjahres, wobei auf Antrag des Mitglieds eine frühere Entlassung ermöglicht werden kann (§ 54 Abs. 4 BNDG). Ein Mitglied kann nur dann aus dem Amt scheiden, wenn ein Nachfolger gewählt wurde (§ 54 Abs. 5 BNDG).

Das PKGr ernennt darüber hinaus einen Präsidenten (und einen Vizepräsidenten), der die Behörde nach Außen vertritt und die Dienstaufsicht ausübt (§ 43 Abs. 4, § 41 Abs. 2 BNDG). Das GeKon besteht aus einem Senat, in dem alle sechs Mitglieder tagen und zwei Kammern mit jeweils drei Mitgliedern, deren Zusammensetzung nach spätestens zwei Jahren zu wechseln ist (§ 49 Abs. 1, 2 BNDG).

b. Rekrutierung der Mitglieder aus obersten Bundesrichtern

Als Mitglieder des GeKons wählbar sind nur Personen, die bis zu ihrer Ernennung Richter am Bundesgerichtshof bzw. am Bundesverwaltungsgericht waren und „in dieser Tätigkeit über langjährige Erfahrung verfügen“, in der Regel über zwanzig Jahre richterliche Erfahrung (§ 43 Abs. 1 BNDG)²²⁴. Die Präsidenten des Bundesgerichtshofs und des Bundesverwaltungsgerichts schlagen dem PKGr hierfür geeignete Kandidaten vor (§ 43 Abs. 3 BNDG).²²⁵

²²³ Die lange Amtszeit hat viele Vorteile: „The members’ tenure can be made longer than the standard electoral period, something which is particularly important as intelligence has, as already mentioned (see above para 90), a relatively long “learning curve”, *Venedig-Kommission*, Report 2015, S. 50 Rn. 229.

²²⁴ Dt. Bundestag, Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND- Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 106.

²²⁵ Nach dem Wortlaut werden dem PKGr die Vorschläge durch die Bundesregierung übermittelt. Es wird zu Recht kritisiert, dass dieser Umweg keinen Sinn ergibt, wenn die Bundesregierung die Wahl nicht beeinflussen möchte, *Markard*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 9. Außerdem wird berechtigterweise gefordert, dass dem PKGr mehrere Bewerber vorgeschlagen werden müssten, damit es tatsächlich eine Auswahl treffen kann, *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 13; *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 21.

Dass nur Richter dieser beiden Gerichte als Mitglieder in Betracht kommen, wird kritisiert. Richter an Obergerwaltungs- und Oberlandesgerichten und Staatsanwälte seien ebenso geeignet.²²⁶

Verfassungsrechtlich problematisch ist die Beschränkung auf diesen Personenkreis jedoch nicht, da bei dem ausgewählten Personenkreis die höchsttrichterlich geforderte besondere fachliche Eignung gegeben ist.²²⁷

c. Stellung als Beamte

Die Mitglieder des GeKons sind Beamte auf Zeit, § 44 Abs. 1 BNDG. Sie werden nach der Besoldungsgruppe B 7 vergütet, wobei der Präsident höher eingestuft wird (B 9, § 46 BNDG). Damit sind die Mitglieder des GeKons hauptberuflich tätig.

d. Mehrheitsfindung

Beschlussfähig sind sowohl der Senat als auch die Kammern dann, wenn mehr als die Hälfte der Mitglieder anwesend sind. Für Entscheidungen ist eine einfache Stimmenmehrheit notwendig, wobei bei Stimmengleichheit die Stimme des Präsidenten ausschlaggebend ist (§ 49 Abs. 3, § 41 Abs. 5 BNDG).

e. Geheimhaltung

Die Beratungen des UKRat sind geheim, seine Mitglieder und Mitarbeiter sind auch für die Zeit nach dem Ende ihrer Tätigkeit zur Geheimhaltung verpflichtet (§ 54 Abs. 1, 2 BNDG). Der Präsident des UKRats kann jedoch eine Aussagegenehmigung erteilen (§ 54 Abs. 3 BNDG²²⁸).

Für alle, die als Mitglieder im oder Mitarbeiter für den UKRat tätig sind, ist eine erfolgreiche erweiterte Sicherheitsüberprüfung vorgeschrieben (§§ 43 Abs. 2, 53 BNDG).

²²⁶ Graulich, GSZ 2021, 121, 128; bzgl. der Richter an OLG auch Löffelmann, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes, S. 21, der auch kritisiert, dass eine „langjährige Erfahrung“ in der Tätigkeit als Richter verlangt wird; ebenso Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12; im Gesetzgebungsverfahren war ursprünglich vorgesehen, dass nur BGH-Richter und Bundesanwälte Mitglieder des UKRat werden können, erst später wurde die Norm um Richter des BVerwG ergänzt.

²²⁷ Vgl. [Teil 2 A. III. 1. b. ii](#)); so auch Alt, Kompensatorische Kontrolle, S. 119.

²²⁸ Geht es um eine Aussage des UKRat-Präsidenten, trifft diese Entscheidung der Vizepräsident, § 54 Abs. 3 S. 3 BNDG.

f. Verfahren

Wie das Verfahren im GeKon abläuft, ist gesetzlich nicht geregelt und die Verfahrensordnung, die sich das GeKon gegeben hat, ist geheim. Das Mitglied des GeKon, Johanna Schmidt-Räntsch, hat den organisatorischen Ablauf der Vorabkontrolle durch das GeKon jedoch in einem Beitrag dargestellt:

Die Aufgaben der beiden Senate werden in einem jährlich im Voraus erstellten Geschäftsverteilungsplan verteilt (§ 5 Abs. 1 GO UKRat). Wenn eine Kammer von der Entscheidungspraxis einer anderen Kammer oder des Senats abweichen möchte oder eine „grundsätzliche Bedeutung“ vorliegt, ist der Senat zuständig (§ 5 Abs. 2 GO UKRat). Der Senat und die Kammern teilen die Berichterstattungen jeweils in eigenen Geschäftsverteilungsplänen auf.

Für jede eingehende Anordnung wird beim GeKon eine Fallakte angelegt. Der Präsident des GeKon prüft nach Eingang der Anordnung, welcher Spruchkörper dafür zuständig ist. Anschließend wird die Fallakte dem zuständigen Berichtersteller übergeben. Nach der Prüfung der Rechtmäßigkeit verfasst der Berichtersteller ein Votum, aus dem sich der Sachverhalt, eine rechtliche Bewertung und ein Vorschlag für die Entscheidung ergeben. Das Votum wird sodann von allen Mitgliedern des Senats oder der zuständigen Kammer beraten.

Wenn die anderen Mitglieder dem Votum zustimmen, wird die Anordnung durch einen Beschluss bestätigt, den alle unterschreiben und der „grundsätzlich“ nicht begründet wird. Der BND enthält anschließend eine Ausfertigung dieses Beschlusses, das Bundeskanzleramt eine beglaubigte Kopie.

Falls der Berichtersteller oder der zuständige Spruchkörper Bedenken bezüglich der Rechtmäßigkeit der Anordnung haben, werden die Verfahrensbeteiligten (i.d.R. nur der BND) schriftlich oder mündlich angehört. Nach der Anhörung beraten die Mitglieder des Spruchkörpers und entscheiden über die Anordnung. Eine Bestätigung der Anordnung (auch mit Vorgaben des Spruchkörpers) ergeht begründungslos als „Formularbeschluss“. Wenn das GeKon die Anordnung als rechtswidrig erachtet, wird die Anordnung nicht bestätigt, aber nicht abgelehnt (§ 23 Abs. 4 S. 2 BNDG). Diese Entscheidung wird begründet. Die nicht bestätigte Anordnung tritt nach der Bekanntmachung der Entscheidung gegenüber dem BND außer Kraft.²²⁹

2. Administratives Kontrollorgan

Die gesetzlichen Vorgaben zum AdKon sind wesentlich knapper.

²²⁹ Alle Ausführungen zum Verfahren sind den Schilderungen von Schmidt-Räntsch entnommen, *Schmidt-Räntsch*, K&R 2022, 34, 39 f.

a. Besetzung

Im Vergleich zu den detaillierten Vorgaben hinsichtlich des GeKons regelt das BNDG die Besetzung des AdKons kaum. Festgelegt ist lediglich, dass es einen Leiter gibt, der über die Befähigung zum Richteramt verfügen muss, der Beamter ist (Besoldungsgruppe B 6) und der den Weisungen des Präsidenten bzw. der Präsidentin unterliegt, § 50 BNDG.

b. Verfahren

Auch die Abläufe im gesetzlich nicht geregelten Verfahren des AdKon hat das Mitglied des GeKon Johanna Schmidt-Räntsch exemplarisch dargestellt:

In der Praxis sind die jeweiligen Kontrollen des AdKon in einzelne Prüfaufträge strukturiert. Die Prüfung beginnt damit, dass der Bearbeiter ein Prüfkonzept erstellt und gemeinsam mit dem Leiter des AdKon entscheidet, welche „Prüftermine mit welchem Prüfungsgegenstand durchgeführt werden sollen“. Die Prüfung wird vorab mit dem BND besprochen, bevor ihm eine schriftliche „Prüfungsankündigung“ zugestellt wird. Daraus ergibt sich der Kontrolltermin, der Kontrollgegenstand, der geplante Ablauf, Ort und Zeit der Kontrollen, „bereits absehbar benötigte“ Unterstützungsbedarfe durch den BND, „Informationen und Unterlagen, die vorab zur Verfügung gestellt werden sollen“ und der zuständige Mitarbeiter des AdKon.

Wenn das AdKon beispielsweise die Umsetzung einer Anordnung des GeKon kontrolliert, gibt es als Kontrollgegenstand in der Prüfungsankündigung unter anderem an, „ob die gesteuerten Suchbegriffe den Vorgaben der Anordnung entsprechen“. Bei dem Prüfungstermin im BND sichten die Vertreter des AdKon dann Stichproben der verwendeten Selektoren und gleichen sie mit der Anordnung ab.²³⁰ Nach Abschluss des Prüfungsvorgangs verfasst der zuständige Mitarbeiter des AdKon einen „schriftlichen Bericht“, den die Leitung des AdKon dann prüft. Anschließend führt das AdKon entweder weitere Kontrollen durch oder informiert das GeKon und den BND über das Ergebnis, bei dem sich entweder eine Beanstandung oder kein Beanstandungsbedarf ergibt.²³¹

V. Distanz

Gem. § 41 Abs. 3, § 44 Abs. 1 S. 3 BNDG ist der UKRat unabhängig und nicht weisungsgebunden. Die Unabhängigkeit wird dadurch gestärkt, dass der UKRat eine oberste Bundesbehörde ist und somit den „die Aufsicht über die Nachrichtendienste

²³⁰ Da die Selektoren in der Anordnung selbst nicht angegeben sind, kann insoweit nur geprüft werden, ob die Suchbegriffe zu diesen Zwecken gesteuert werden durften.

²³¹ Schmidt-Räntsch, K&R 2022, 34, 40 f.

führenden Ministerien organisatorisch und statusmäßig“ gleichgestellt ist.²³² Die Unabhängigkeit der Mitglieder wird auch dadurch gestärkt, dass sie für zwölf Jahren gewählt werden und nicht erneut wählbar sind.²³³ Allerdings gibt es einige Normen, die an der vollständigen Unabhängigkeit Zweifel aufkommen lassen.

Erstens stellt sich die Frage, wieso der UKRat die Bundesregierung anhören muss, bevor er seine Geschäfts- und Verfahrensordnung erlassen darf (§ 41 Abs. 5 S. 1 BNDG).²³⁴ Der Gesetzgeber betont jedoch, dass es sich dabei nicht um einen Zustimmungsvorbehalt handelt, sondern dass die Regelung dazu diene, die Zusammenarbeit zu erleichtern und unter anderem einen „Gleichlauf“ sicherheitsrechtlicher Standards zu ermöglichen.²³⁵

Zweitens ist das Bundeskanzleramt anzuhören, bevor der UKRat das PKGr über seine Tätigkeit informiert (§ 55 Abs. 2, 3 BNDG).²³⁶ So soll verhindert werden, dass die Third Party Rule verletzt wird, wenn der Bericht Inhalte enthält, die nicht der alleinigen Verfügungsberechtigung des BND unterliegen.²³⁷ Wieso der UKRat nicht in der Lage sein soll, solche Daten sicher zu erkennen und nicht in den Bericht aufzunehmen, ist unklar. Wenn entsprechend der Gesetzesbegründung die Einflussnahme des Bundeskanzleramts auf den Bericht tatsächlich auf diesen Aspekt begrenzt ist, wird die Unabhängigkeit dadurch jedoch nicht (über Gebühr) eingeschränkt.

Drittens entspricht der Dienstsitz des UKRat gem. § 41 Abs. 6 BNDG dem Dienstsitz des BND. Sollte der UKRat in den Räumlichkeiten des BND arbeiten, würde die Unabhängigkeit durch die räumliche Nähe zumindest gefährdet (Gefahr der Fraternalisierung zwischen Kontrolleur und Kontrolliertem).²³⁸ Bei dem aktuellen Dienstsitz des UKRat, der sich in Berlin Mitte befindet, handele es sich um ein Provisorium, die Sitzungen fänden nicht dort, sondern in einer abhörsicheren Außenstelle des BND

²³² *Löffelmann/Zöller*, Nachrichtendienstrecht, S. 261; Ähnlich auch *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 11.

²³³ *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 16; Wegen dem Phänomen der „agency capture“ kommt Cameron zu folgendem Schluss: „The watchdogs thus have to be replaced after a while“, *Cameron*, National Security, S. 167 f.

²³⁴ *BfDI*, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 11.

²³⁵ Dr. Bundestag, Drs. 19/26103, Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 103.

²³⁶ Kritisch insoweit *BfDI*, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 11.

²³⁷ Dr. Bundestag, Drs. 19/26103, Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 112.

²³⁸ So werde die notwendige Distanz „faktisch unterlaufen“, *BfDI*, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 11.

statt.²³⁹ Der UKRat sollte Räumlichkeiten außerhalb der Liegenschaften des BND zur Verfügung gestellt bekommen.

Viertens wird kritisiert, dass der UKRat „Aufgaben der Personalverwaltung und Personalwirtschaft auf das Bundeskanzleramt oder ein Bundesministerium übertragen“ kann (§ 57 Abs. 2 S. 1 BNDG).²⁴⁰ Diese Norm solle „die zukünftig kleinste oberst[e] Bundesbehörde“ „organisationsrechtlich“ entlasten, die Personalhoheit habe jedoch weiterhin der UKRat.²⁴¹ Dabei muss sichergestellt werden, dass der UKRat seine Mitarbeiter selbst auswählt, um die notwendige Distanz zum BND und dem Bundeskanzleramt zu wahren. Demgegenüber erscheint die Übertragung von Verwaltungsaufgaben unproblematisch.

Das Bundesverfassungsgericht hat geurteilt, dass die Kontrolleure „wirksam“ von Einflussnahmen „abgeschirmt“ werden und „vollständig unabhängig“ sein müssen.²⁴² Dem werden die angesprochenen Normen nur bei restriktiver Auslegung gerecht. Zusätzlich sollte § 41 Abs. 6 BNDG klarstellend um einen Satz ergänzt werden, wonach der UKRat nicht beim BND angesiedelt werden darf.

VI. Modalitäten

Die Vorabkontrolle erstreckt sich auf jede einzelne Maßnahme. Die Rechtskontrolle durch das GeKon gem. § 42 Abs. 2, 4 BNDG erfolgt laufend. Dies ergibt sich aus § 42 Abs. 5 BNDG, der den BND verpflichtet, „dem gerichtsähnlichen Kontrollorgan den Kontrollgegenstand unverzüglich vorzulegen“. Würde es sich um eine stichprobenartige Kontrolle handeln, wäre eine unverzügliche Vorlagepflicht nicht notwendig gewesen. Auch der Gesetzesentwurf zur Schaffung des UKRats legt dies nahe, da bezüglich des AdKons von „stichprobenmäßigen“ Kontrollen gesprochen wird²⁴³, während dieser Begriff im Zusammenhang mit den Erläuterungen zu § 42 BNDG nicht zu finden ist.

²³⁹ <https://www.tagesschau.de/investigativ/ndr-wdr/unabhaengiger-kontrollrat-101.html> (abgerufen am 31.8.2024).

²⁴⁰ Markard, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 9; BfDI, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 11.

²⁴¹ Dt. Bundestag, Drs. 19/26103, Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.01.2021, S. 114.

²⁴² BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 281.

²⁴³ Dt. Bundestag, Drs. 19/26103, Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.01.2021, S. 110.

Das GeKon trifft seine Entscheidungen mit einfacher Mehrheit, bei Stimmengleichheit entscheidet die Stimme des Vorsitzenden (§ 4 Abs. 2 GO UKRat²⁴⁴).

VII. Initiative

Das GeKon genehmigt Anordnungen, die der BND vorlegt (vgl. z.B. § 23 Abs. 4, 7 BNDG). Das gilt auch für die ex post-Kontrolle (§ 42 Abs. 5 BNDG). Wenn es um Beanstandungen geht, wird er auf Initiative des administrativen Kontrollorgans hin tätig (§ 52 Abs. 3 BNDG). Demgegenüber prüft das AdKon eigeninitiativ.²⁴⁵

VIII. Kontrollmittel zur Informationsgewinnung

Dem UKRat wurden unterschiedliche Kontrollmittel verliehen (1.), die teilweise jedoch nicht weit genug gehen (2.).

1. Kontrollmittel

Der BND muss den UKRat bei seinen Aufgaben unterstützen (§ 56 Abs. 1 BNDG). Im Rahmen seiner Kontrollbefugnis kann der UKRat vom BND erstens verlangen, dass ihm „Akten oder andere in amtlicher Verwahrung befindliche Schriftstücke, soweit im Einzelfall ein berechtigtes Interesse besteht auch im Original, und in Dateien gespeicherte Daten“ zur Verfügung gestellt werden (§ 56 Abs. 2 BNDG). Zweitens kann er jederzeit Zutritt zu sämtlichen Dienststellen und Zugang zu sämtlichen informationstechnischen Systemen verlangen²⁴⁶, allerdings unter der Einschränkung, dass diese „in alleiniger Verfügungsberechtigung“ des BND stehen „und dies für die Durchführung der Kontrolle erforderlich ist“ (§ 56 Abs. 3 BNDG). Stünden diese nicht in der alleinigen Verfügungsberechtigung des BND, ergreife das Bundeskanzleramt auf Verlangen des UKRats „geeignete Maßnahmen“, um dem UKRat den Zutritt bzw. Zugang zu ermöglichen. Drittens kann der UKRat Mitarbeiter des BND befragen oder von ihnen schriftliche Auskünfte einholen, wobei diese „unverzüglich“ antworten und dabei „vollständige und wahrheitsgemäße Angaben“ machen müssen (§ 56 Abs. 4 BNDG).

²⁴⁴ Unabhängiger Kontrollrat, Bekanntmachung der Geschäftsordnung v. 12.12.2021, BAnz AT 27.12.2021 B4.

²⁴⁵ Dt. Bundestag, Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.01.2021, S. 50 u.a.

²⁴⁶ Im Jahr 2022 habe das AdKon beispielsweise „regelmäßig Vor-Ort-Kontrollen beim BND durchgeführt“, *Hoch/Schmidt-Räntsch/Brunst*, NVwZ 2023, 712, 714, 716.

2. Verfassungsrechtliche Bedenken

Ob diese Ausgestaltung die verfassungsrechtlichen Anforderungen erfüllt, ist fraglich.

a. Gesteigerte Anforderung für die Einsichtnahme in Originale

Problematisch ist zunächst, dass der UKRat Akten nur im Original einsehen darf, wenn „im Einzelfall ein berechtigtes Interesse“ daran besteht. Wer aber darf entscheiden, ob das Interesse im Einzelfall „berechtigt“ ist? Die Gesetzesbegründung enthält dazu keine Ausführung. Die Formulierung erweckt den Eindruck, dass der UKRat gegenüber dem BND zumindest zu einer detaillierten Begründung verpflichtet ist. Das Bundesverfassungsgericht hat jedoch entschieden, dass der Kontrolleur „umfassend Zugang zu allen Unterlagen“ haben muss²⁴⁷; Einschränkungen hat es nicht vorgesehen. Als eine solche Einschränkung denkbar gewesen wäre beispielsweise eine Formulierung, wonach die Unterlagen zumindest in Kopie herauszugeben sind. Eine Unterscheidung von Schriftstücken in Originale und Kopien kennt die vergleichbare Befugnis der G 10-Kommission nicht (§ 15 Abs. 5 S. 3 Nr. 2 G 10). Dass für die Einsichtnahme in Original-Akten und Dokumente ein berechtigtes Interesse geltend gemacht werden muss, ist mit der Rechtsprechung des Bundesverfassungsgerichts nicht vereinbar. Ob eine Kopie ausreichend ist, sollte allein der UKRat entscheiden dürfen.

b. Ausnahme vom Zutrittsrecht bei „Ausnahmesituationen“

In Situationen gem. § 56 Abs. 3 BNDG, wenn Dienststellen oder informationstechnische Systeme nicht in alleiniger Verfügungsberechtigung des BND stehen und der UKRat das Bundeskanzleramt um „geeignete Maßnahmen“ gebeten hat, um einen Zugang zu ermöglichen, kann das Bundeskanzleramt dieses Ersuchen laut der Begründung des Gesetzesentwurfs offenbar ablehnen. Demnach sei eine „entsprechende Ausnahmesituation, die nur eine Unterrichtung eines sehr engen Personenkreises“ ermögliche, „nicht gänzlich auszuschließen“. Das Bundeskanzleramt müsse seine Entscheidung begründen und mit dem UKRat nach einer „angemessenen Unterrichtungsmöglichkeit suchen, die trotz der Ausnahmesituation die erforderliche Rechtskontrolle ermöglicht“. ²⁴⁸

Die Vorgabe des Bundesverfassungsgerichts, wonach den Kontrolleuren „jederzeit[er] Zutritt zu gewähren“ ist, lässt jedoch keinen Spielraum für Ausnahmen, die

²⁴⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 Rn. 290; vgl. Teil 2 A. III. 1. b. gg).

²⁴⁸ Dt. Bundestag, Drs. 19/26103, Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.01.2021, S. 113 f.

Third Party Rule darf der umfassenden Rechtskontrolle ausdrücklich nicht entgegengehalten werden.²⁴⁹

Dass das Zutrittsrecht im Ausnahmefall verweigert werden kann, soweit alternativ andere Unterrichtungsmöglichkeiten angeboten werden, ist mit der geltenden Rechtsprechung nicht vereinbar.

c. Kein Schutz gegen Falschaussagen

Darüber hinaus wird zu Recht kritisiert, dass gegenüber dem UKRat getätigte Falschaussagen nicht sanktioniert werden. Der UKRat sei insoweit „schlechter gegen Fehlinformationen und Falschaussagen geschützt als ein normales Gericht oder ein Parlamentarischer Untersuchungsausschuss“. Weil der UKRat zur Aufgabenerfüllung darauf angewiesen ist, die Wahrheit zu erfahren, werden die Vorgaben an eine unabhängige gerichtsähnliche Kontrolle insoweit nicht erfüllt.²⁵⁰

d. Keine Zwangsbefugnisse zur Durchsetzung von § 56 BNDG

Darüber hinaus fehlen dem UKRat Befugnisse zur Durchsetzung der Unterstützungspflicht aus § 56 BNDG, was dazu führt, dass vor allem Personen, die nicht für den BND arbeiten, wie beispielsweise V-Leute, Zeugen und Sachverständige nicht zu einer Aussage gezwungen werden können.²⁵¹ In diesem Zusammenhang wird zudem kritisiert, dass das Verfahren gem. § 41 Abs. 5 S. 1 Nr. 2 BNDG durch den UKRat festgelegt werden soll, anstatt es – wie bei Gerichten üblich – gesetzlich zu regeln.²⁵² Daher wird vorgeschlagen, das Beweisrecht der VwGO oder der StPO entsprechend anzuwenden.²⁵³

²⁴⁹ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 Rn. 290, 294; vgl. zu dieser Problematik bei Kontrollen durch die BfDI schon *BfDI*, Sachstandsbericht 2016.

²⁵⁰ Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12; Gärditz, GSZ 2021, 905, 912; ähnlich Dietrich, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 21; Bäcker, Beschwerdeschrift BNDG II, S. 105; Vogt, DöV 76 (2023), 689, 698.

²⁵¹ Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12, Gärditz, GSZ 2021, 905, 911; dem zustimmend Graulich, GSZ 2021, 121, 128; Markard, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 10; Bäcker, Beschwerdeschrift BNDG II, S. 105; Vogt, DöV 76 (2023), 689, 698.

²⁵² Dietrich, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 21. Diese internen Verfahrensregelungen haben keine außenrechtliche Wirkung und verletzen den Gesetzesvorbehalt, Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12; Bäcker, Beschwerdeschrift BNDG II, S. 105.

²⁵³ Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12; erachtet dies demgegenüber als „für die verfassungsrechtlich geforderte Effektivität nicht erforderlich“, Alt, Kompensatorische Kontrolle, S. 213 f.

IX. Kontrollergesultfolgen

Die Kontrollergesultfolgen unterscheiden sich je nachdem, ob das GeKon oder das AdKon tätig werden.

1. Gerichtsähnliches Kontrollorgan

Das GeKon verfügt über eine „abschließende Entscheidungszuständigkeit“. ²⁵⁴ So treten beispielsweise Anordnungen, deren Rechtmäßigkeit es nicht bestätigt, außer Kraft (§ 23 Abs. 4 S. 2, § 23 Abs. 7 S. 2, § 37 Abs. 4 S. 2 BNDG). Diese „Verweigerung der verfahrenstechnisch notwendigen Bestätigung der Rechtmäßigkeit etlicher BND-Maßnahmen im Bereich der strategischen Fernmeldeaufklärung“ ist das „schärfst[e] Schwert“ des UKRats. ²⁵⁵

Für die nachträglichen Kontrollen des GeKon wurden keine Kontrollergesultfolgen normiert. Allerdings hat das GeKon in der Praxis die Möglichkeit, anzudrohen, dass es Genehmigungen nicht verlängert oder zukünftig verweigert. Deshalb ist davon auszugehen, dass die nachträglichen Kontrollen des GeKon trotzdem wirksam sind. ²⁵⁶

2. Administratives Kontrollorgan

Das AdKon hat keine Entscheidungszuständigkeit, sondern lediglich ein Beanstandungsrecht gem. §§ 1 Abs. 3, 52 BNDG.

Das Beanstandungsverfahren ist mehrstufig konzipiert: Stellt das AdKon einen rechtswidrigen Zustand fest, muss es den BND zunächst anhören, bevor es eine Beanstandung aussprechen darf (§ 52 Abs. 1 BNDG).

Anschließend gibt es mehrere Optionen. Entweder das AdKon stellt das Verfahren ein oder der BND stimmt ihm zu und verspricht, dass rechtswidrige Verhalten einzustellen. Dann kann das AdKon von der Beanstandung absehen, soweit der „rechtswidrige Zustand keine erhebliche Bedeutung hat“. Wenn der rechtswidrige Zustand demgegenüber von erheblicher Bedeutung ist, erlässt das AdKon einen schriftlichen, begründeten Beanstandungsbescheid. Falls der BND den Zustand noch nicht behoben

²⁵⁴ Dt. Bundestag, Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.01.2021, S. 103.

²⁵⁵ Ader, Hdb. Sicherheits- und Staatsschutzrecht, 612, 659 Rn. 162.

²⁵⁶ Geht demgegenüber davon aus, dass sich „die gesamte nachträgliche Kontrolle des gerichtsähnlichen Gremiums (...) auf einen bloßen Soll-Ist-Vergleich beschränkt“, Alt, Kompensatorische Kontrolle, S. 124.

hat, wird ihm eine angemessene Abhilfefrist gestellt. Wenn der BND die Rechtswidrigkeit dann behebt, ergeht ein Bescheid, dass dem rechtswidrigen Zustand nach Beanstandung abgeholfen wurde.²⁵⁷

Wenn der rechtswidrige Zustand nicht innerhalb einer durch das Gremium gesetzten, angemessenen Frist behoben wurde, kann darüber hinaus eine Beanstandung gegenüber dem Bundeskanzleramt ausgesprochen werden, das dazu Stellung nehmen muss (§ 52 Abs. 2 BNDG). Wenn der rechtswidrige Zustand dann beendet wird, ergeht ein Bescheid, dass er nach Beanstandung abgestellt wurde. Ändert das AdKon nach der Stellungnahme des Bundeskanzleramts hingegen seine Einschätzung, stellt es das Verfahren mit einem förmlichen Bescheid ein. Wenn das Bundeskanzleramt nicht innerhalb von drei Monaten Stellung nimmt oder das AdKon nach der Stellungnahme weiterhin an der Beanstandung festhalten möchte, kann es die Beanstandung dem GeKon zur abschließenden Entscheidung vorlegen (§ 52 Abs. 3 BNDG, aktuell ist der Senat dafür zuständig). In dieser Vorlage erörtert das AdKon die Ursachen der Beanstandung, das bisherige Verfahren und die (von ihm kommentierten) Vorträge von BND und Bundeskanzleramt. Diese Vorlage wird dem BND und dem Bundeskanzleramt zur (erneuten) Stellungnahme vorgelegt (§ 52 Abs. 4 S. 1 BNDG). Anschließend kann eine mündliche Besprechung anberaumt werden. Wenn die Beanstandung rechtmäßig ausgesprochen wurde, entscheidet das GeKon, das ihr innerhalb einer bestimmten Frist abzuhelpen ist, ansonsten stellt es das Verfahren ein (§ 54 Abs. 4 S. 2 BNDG).²⁵⁸

Diese Ausgestaltung ist noch im Rahmen der Vorgaben des Bundesverfassungsgerichts. Allerdings wird zu Recht angemahnt, dass insgesamt drei Anhörungen erfolgen müssen, wodurch das Beanstandungsverfahren „zu langwierig und schwerfällig“ wird.²⁵⁹ Insoweit bietet es sich an, die Regelung so anzupassen, dass die Beanstandung nach dem BND nicht erst noch dem Bundeskanzleramt, sondern direkt dem GeKon vorgelegt wird.²⁶⁰

3. Bericht an das Parlamentarische Kontrollgremium und den Bundestag

Darüber hinaus berichtet der UKRat dem PKGr im Abstand von höchstens sechs Monaten über seine Arbeit (§ 55 Abs. 1 BNDG). Dadurch soll sichergestellt werden, dass das PKGr über alle notwendigen Informationen verfügt. Insoweit soll der UKRat das

²⁵⁷ *Schmidt-Räntsch*, K&R 2022, 34, 41.

²⁵⁸ *Schmidt-Räntsch*, K&R 2022, 34, 41.

²⁵⁹ *Markard*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 10; *Wetzling* warnt vor einem „Beanstandungs-marathon“, *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 8; *Wetzling*, Bedingt kontrollfähig, S. 15 f.

²⁶⁰ *Hoch et al.*, Diskussionsentwurf, S. 8, 34.

PKGr nach dem Willen des Gesetzgebers „vor allem über strukturelle Probleme informieren“, aber nicht über „die Einzelheiten von Vorgängen“.²⁶¹

§ 58 Abs. 1 BNDG legt zusätzlich fest, dass sich der UKRat mit dem PKGr regelmäßig „im Rahmen der jeweiligen Kontrollzuständigkeit über allgemeine Angelegenheiten der Kontrolltätigkeit“ austauschen kann, soweit dabei die Geheimhaltungsvorschriften gewahrt bleiben. Die Begrenzung auf allgemeine Angelegenheiten soll verhindern, dass in einem Austausch über konkrete Vorgänge Informationen von ausländischen Partnerdiensten geteilt werden und damit die Third Party Rule verletzt wird. Mit Blick auf die Vorgaben des Bundesverfassungsgerichts, wonach die Third Party Rule die Kontrolle des UKRats nicht behindern darf²⁶², ist es richtig, dass die Austauschmöglichkeiten mit dem PKGr begrenzt sind, weil es als „Dritter“ angesehen wird und man ansonsten riskieren würde, dass auch der UKRat nicht alle notwendigen Informationen erhält.²⁶³

Das PKGr wird darüber hinaus „in abstrakter Weise“ über Beanstandungen unterrichtet, die das GeKon ausgesprochen hat; anschließend soll der Bundestag informiert werden (§ 55 Abs. 3 BNDG).

Der Bericht an das PKGr und den Bundestag und der Austausch mit dem UKRat ermöglichen, dass politische Konsequenzen gezogen werden können.²⁶⁴

X. Fachkompetenz und Ressourcen

Das GeKon besteht aus sechs ehemaligen obersten Bundesrichtern.²⁶⁵ Zur Besetzung des AdKons enthält das Gesetz keine Vorgaben.

Dem UKRat ist „die für die Erfüllung seiner Aufgaben angemessene Personal- und Sachausstattung zur Verfügung zu stellen“ (§ 57 Abs. 1 BNDG). Laut dem Gesetzesentwurf sind in diesem Zusammenhang „Personal-, Sacheinzel- und Gemeinkosten für insgesamt 62 Planstellen/Stellen (davon 27 im höheren Dienst, 18 im gehobenen

²⁶¹ *Meinel*, Stellungnahme zu zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 3.

²⁶² Vgl. [Teil 2 A. III. 1. b. II](#).

²⁶³ So auch *Meinel*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 4.

²⁶⁴ *Meinel*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 4; zur Information des Bundestags durch das politische Kontrollorgan, *Masing*, Nachrichtendienste, 3, 14: „Man wird insoweit darüber nachdenken müssen, den Kontrollinstanzen wenigstens das – eventuell verfahrensrechtlich eingeschränkte – Recht einzuräumen, jedenfalls in abstrahierter, die konkrete Aufgabenwahrnehmung nicht beeinträchtigender Weise etwaige Misstände dem Parlament und der Öffentlichkeit mitzuteilen. Soll Kontrolle eine Bedeutung haben, ist schwer vorstellbar, dass unliebsame Ergebnisse wie im Märchen als Geheimnis des Königs gehandelt werden müssen, die nur in ein Loch im Wald gerufen werden dürfen.“

²⁶⁵ Vgl. [Teil 3 C. IV. 1. b](#).

Dienst und 17 im mittleren Dienst)“ in Höhe von circa 11,6 Mio. Euro jährlich eingeplant.²⁶⁶ Damit verfügt der UKRat über enorme personelle und sachliche Ressourcen. Die Anforderungen des Bundesverfassungsgerichts, wonach „ausreichende personale und sachliche Mittel“ bereitzustellen sind, sind damit eindeutig erfüllt.

Im Gegensatz zu § 15 Abs. 3 S. 2 G 10 enthält das BNDG keine Klarstellung dahingehend, dass am UKRat Mitarbeiter mit technischem Sachverstand anzustellen sind. Im Rahmen seiner Ausführung zur Besetzung des richterähnlichen Kontrollgremiums hatte das Bundesverfassungsgericht ausgeführt, „dass Fachwissen aus anderen juristischen Berufen und technischer Sachverstand nützlich“ sein könnten und daher „Nichtjuristen als Gremienmitglieder“ vorgesehen oder andere Möglichkeiten genutzt werden könnten, um „technische Expertise einzubinden“.²⁶⁷ Bezogen auf das administrative Kontrollorgan beließ es das Bundesverfassungsgericht nicht bei Empfehlungen, sondern forderte, dass die Berücksichtigung von Personen „mit informationstechnischen Kenntnissen“ erforderlich ist.²⁶⁸

Deshalb sollte § 57 Abs. 1 BNDG um eine entsprechende Formulierung ergänzt werden.²⁶⁹

Außerdem wird kritisiert, dass der UKRat weder Sachverständige noch den Ständigen Bevollmächtigten (§ 5a PKGrG) anhören dürfe.²⁷⁰ Diese Forderung ist zwar sinnvoll, verfassungsrechtlich aber nicht zwingend.

XI. Kontrollniveau

Innerhalb des UKRat ist wegen der Zusammenarbeitspflicht der beiden Gremien ein offener Austausch gewährleistet (§ 51 Abs. 1, 2 BNDG).

Darüber hinaus ist der UKRat – im Einklang mit den Vorgaben der Rechtsprechung²⁷¹ – dazu verpflichtet, das PKGr mindestens alle sechs Monate „über seine Tätigkeit“ zu unterrichten (§ 55 Abs. 1 BNDG). Darüber hinaus berichtet der UKRat dem PKGr „in abstrakter Weise und nach Anhörung des Bundeskanzleramts“ über Beanstandungen, über die das GeKon entschieden hat (§ 55 Abs. 3 BNDG).

²⁶⁶ Dr. Bundestag, Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.01.2021, S. 3.

²⁶⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 Rn. 287.

²⁶⁸ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 Rn. 284 f.

²⁶⁹ Dietrich, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 22: „Der Gesetzesentwurf gibt hierauf keine Antwort.“

²⁷⁰ Dietrich, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 22.

²⁷¹ Vgl. [Teil 2 A. III. 1. b. kk](#).

Das Gesetz zur Schaffung des UKRats aus dem März 2021 hat offengelassen, ob das PKGr zukünftig den UKRat kontrollieren soll.²⁷² Dagegen spricht, dass die politische Kontrolle durch das PKGr nach der Rechtsprechung des Bundesverfassungsgerichts von der Rechtskontrolle durch den UKRat zu trennen ist²⁷³, auch, weil die Third Party Rule dem UKRat nicht entgegengehalten werden kann, dem Parlamentarischen Kontrollgremium aber schon²⁷⁴.

Ein Austausch über allgemeine Angelegenheiten ist auch zwischen dem UKRat, der G 10-Kommission und dem BfDI vorgesehen (§ 58 Abs. 3 BNDG). Die Begrenzung auf „allgemeine Angelegenheiten“ verhindert jedoch eine inhaltliche Zusammenarbeit, mit deren Hilfe Kontrolllücken und doppelte Kontrollen vermeidbar wären.²⁷⁵ Das ist jedenfalls bei der Kooperation mit dem BfDI, der wie der UKRat im Bereich der Exekutive angesiedelt ist²⁷⁶, nicht nachvollziehbar. Anders als beim Austausch mit dem PKGr²⁷⁷ droht insoweit keine Verletzung der Third Party Rule. Auch gegenüber der G 10-Kommission darf der Third Party Rule-Einwand nicht erhoben werden.²⁷⁸

Gegen die Begrenzung des Austauschs auf allgemeine Angelegenheiten spricht auch, dass dann die Umsetzung des in der Rechtsprechung des Bundesverfassungsgerichts angelegten Kontroll-Gesamtüberblicks²⁷⁹ nicht möglich ist.

XII. Barrieren

Denkbaren Ressourcenbarrieren begegnet § 57 Abs. 1 BNDG, indem er normiert, dass dem UKRat eine „angemessene Personal- und Sachausstattung“ zur Verfügung stehen muss.

Darüber hinaus muss der UKRat nach den Vorgaben des Bundesverfassungsgerichts so organisiert sein, dass die Third Party Rule für ihn keine Kontrollbarriere darstellen kann. Die Vereinbarkeit der Kontrolltätigkeit mit der Third Party Rule wird vor

²⁷² Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 14 ff.; Barczak, KritV 2021, 91, 129; a.A. Meinel, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 3: „Auch ist der UK-Rat nach der Konzeption des Gesetzes insofern relativ nah am Parlament als er selbst nicht Objekt der Kontrolle des PKGr sein soll“.

²⁷³ Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 14 ff; Barczak, KritV 2021, 91, 129.

²⁷⁴ Meinel, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 4; Barczak, KritV 2021, 91, 129.

²⁷⁵ BfDI, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 10; darüber hinaus schlägt Wetzling weitere Zusammenarbeitsmöglichkeiten vor, Wetzling, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15.

²⁷⁶ Vgl. [Teil 1 A. I. 1. b.](#)

²⁷⁷ Vgl. [Teil 3 C. IX. 3.](#)

²⁷⁸ Vgl. aber [Teil 3 B. XII. 2.](#)

²⁷⁹ Vgl. [Teil 2 A. II. 5. c.](#)

allem durch die Behördenstruktur des UKRat sichergestellt: Als oberste Bundesbehörde ist er Teil der Exekutive und somit kein „Dritter“ im Sinne der Third Party Rule.²⁸⁰ Vereinzelt droht dennoch eine Wirkung der Third Party Rule als Kontrollbarriere, wenn der Zugang zu informationstechnischen Systemen bzw. der Zugang zu Diensträumen verwehrt werden kann, weil keine alleinige Verfügungsberechtigung des BND besteht²⁸¹.

D. Rechtskontrolle der Datenschutzbeauftragten

Der Bundesbeauftragte für den Datenschutz (BfDI) und die Landesdatenschutzbeauftragten sind dafür zuständig, Datenverarbeitungen durch die Nachrichtendienste zu kontrollieren.

I. Folge der generellen Verneinung des Anwendungsbereichs von Unionsrecht

Weil der Anwendungsbereich des Unionsrechts nach der (noch) herrschenden Meinung im Bereich der Nachrichtendienste grundsätzlich verneint wird²⁸², werden die Vorgaben der DSGVO oder der JIRL in den Fachgesetzen nicht beachtet²⁸³. Daraus folgt beispielsweise, dass die Datenschutzbeauftragten gegenüber den Nachrichtendiensten de lege lata nicht über die weitreichenden unionsrechtlichen Abhilfebefugnisse verfügen²⁸⁴.

II. Datenschutzkontrolle des Einsatzes nachrichtendienstlicher Mittel

Im Folgenden wird dargestellt, wie die Rechtsgrundlagen der Nachrichtendienstkontrolle durch die Datenschutzbeauftragten ausgestaltet sind.

²⁸⁰ Dietrich, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 24; Graulich, GSZ 2021, 121, 128; Der UKRat ist zwar „organisatorisch an die Exekutive angebunden“, allerdings nicht in deren „Verwaltungsorganisation und -hierarchie eingebunden“, funktional handle es sich aber um Judikative, Barczak, KritV 2021, 91, 128.

²⁸¹ Vgl. [Teil 3 C. VIII. 2. b.](#)

²⁸² Vgl. [Teil 2 B. II. 1.](#)

²⁸³ Vereinzelt sind die Normen jedoch entsprechend anwendbar, vgl. [Teil 3 D. II. 6. a.](#)

²⁸⁴ Vgl. [Teil 3 D. II. 6.](#), anders jedoch im Saarland und in Bremen.

1. Maßstab der Kontrolle und Rechtsgrundlagen

Die Datenschutzbeauftragten sind – wie auch die G 10-Kommissionen und der UKRat – für die Kontrolle der Rechtmäßigkeit einer Datenverarbeitung zuständig.

a. Rechtsgrundlage auf der Bundesebene

Die Zuständigkeit des BfDI für die Nachrichtendienstkontrolle ergibt sich aus § 28 Abs. 2 BVerfSchG (i.V.m. § 63 BNDG bzw. § 13a MADG): Demnach kontrolliert die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beim BfV (sowie bei BND und MAD) die Einhaltung der Vorschriften über den Datenschutz.

b. Rechtsgrundlagen auf der Landesebene

Auf der Landesebene ist die Zuständigkeit der Landesdatenschutzbeauftragten teilweise wie auf der Bundesebene geregelt.²⁸⁵ In anderen Fachgesetzen werden häufig bestimmte Normen des LDSG für anwendbar erklärt, aus denen sich unter anderem die Zuständigkeit der Datenschutzbeauftragten ergibt.²⁸⁶ Im Saarland folgt die Zuständigkeit unmittelbar aus dem Landesdatenschutzgesetz (§ 3 Abs. 1 SDSG).

Vereinzelt ist die Zuständigkeit allerdings nicht eindeutig geregelt. Besonders widersprüchlich ist die Gesetzeslage in Mecklenburg-Vorpommern: Dort regelt § 2 Abs. 3 DSG MV, dass das Landesdatenschutzgesetz den Verfassungsschutz nur bindet, soweit er „allgemeine Verwaltungsaufgaben“ wahrnimmt. Gem. § 30 VerfSchG MV sind jedoch nur bestimmte, abschließend aufgezählte Normen des DSG MV auf den Verfassungsschutz nicht anwendbar, was im Umkehrschluss bedeutet, dass die restlichen Normen anzuwenden sind. Noch verworrener wird die Rechtslage, wenn man berücksichtigt, dass § 30 VerfSchG MV auf die alte Version des Datenschutzgesetzes verweist, weshalb nach geltendem Recht einzelne Verweise ins Leere gehen.²⁸⁷ Auf diese Unklarheiten bei der Zuständigkeit des Datenschutzbeauftragten angesprochen, hat das zuständige Ministerium ausgeführt, dass die Verweise „aus unterschiedlichen Gründen“ bisher nicht angepasst wurden, eine Reform für 2023 jedoch geplant sei.²⁸⁸ Dass die Verweise im Verfassungsschutzgesetz über einen Zeitraum von mehr als fünf Jahren

²⁸⁵ § 17 BWLVSG; § 30 Abs. 1 LVerfSchG RP; § 15 Abs. 2 VSG NRW; § 23b Abs. 2 HmbVerfSchG; § 33a Abs. 1 NVerfSchG; § 31 BremVerfSchG; § 21 BremDSGVOAG; § 39 Abs. 1 SächsVSG; § 32a Abs. 2 VSG Bln; Art. 32 Abs. 2 BayVSG.

²⁸⁶ § 15 Abs. 1 Nr. 1 HVSG; § 13 Abs. 1 HDSIG; § 36 ThürVerfSchG; § 2 Abs. 1, § 7 Abs. 2–4 ThürDSG; § 2 Abs. 7 Nr. 1, § 17 LDSG SH; § 27 Abs. 1 Nr. 1 BbgVerfSchG; § 18 Abs. 1 BbgDSG; § 30 S. 1 VerfSchG-LSA; § 22 Abs. 1 DSG-LSA in der Fassung der Bekanntmachung vom 13. Januar 2016.

²⁸⁷ § 25 DSG MV auf den § 30 VerfSchG MV verweist, gibt es nicht.

²⁸⁸ Bis zum August 2024 ist eine Anpassung nicht erfolgt.

seit der Novelle des DSG nicht angepasst worden sind, ist aus rechtsstaatlicher Perspektive nicht hinnehmbar. Da die externe Datenschutzkontrolle verfassungsrechtlich zwingend erforderlich ist, sollte die Zuständigkeit des LfDI für die Kontrolle des Verfassungsschutzes bis zu einer gesetzlichen Klarstellung aus § 30 VerfSchG MV i. V. m. § 19 Abs. 1 S. 2 DSG MV hergeleitet werden. Solange keine einfach-rechtliche Ausgestaltung vorliegt, kann die Notwendigkeit der Datenschutzkontrolle aus dem Recht der informationellen Selbstbestimmung hergeleitet werden.

c. Rechtmäßigkeitskontrolle als wesentlicher Bestandteil der Datenschutzkontrolle

Die Bund-Länder-AG des Innenministeriums, die zur Analyse der Konsequenzen aus der Entscheidung des Bundesverfassungsgerichts zum Bayerischen Verfassungsschutzgesetz²⁸⁹ eingesetzt wurde, schreibt: „Aufgabe des BfDI/ LfDI ist nach dem Willen des Gesetzgebers die Kontrolle der Einhaltung von Datenschutzregelungen und somit die Prüfung etwaiger Verletzungen individueller Rechte bei der Verarbeitung personenbezogener Daten; [er] prüft nicht die Rechtmäßigkeit der Maßnahme an sich.“²⁹⁰ Während der erste Halbsatz zutrifft, ist die Folgerung des zweiten Halbsatzes nicht überzeugend, da sie die Struktur des Datenschutzrechts verkennt.

Denn die Mehrheit der durch die Datenschutzbeauftragten zu kontrollierenden nachrichtendienstlichen Datenverarbeitungen sind Grundrechtseingriffe in das allgemeine Persönlichkeitsrecht der betroffenen Personen. Diese Grundrechtseingriffe sind wegen des Gesetzesvorbehalts nur rechtfertigbar, wenn sie auf einer Rechtsgrundlage beruhen, deren Grenzen eingehalten wurden, wenn sie also rechtmäßig erfolgt sind. Wenn der Datenschutzbeauftragte prüft, ob bei der Verarbeitung personenbezogene Rechte verletzt wurden, muss er folglich stets prüfen, ob die Verarbeitung aufgrund einer einschlägigen Rechtsgrundlage rechtmäßig erfolgt ist.

Der Datenschutzbeauftragte prüft nicht „nur“ die Rechtmäßigkeit, sondern auch eigenständige Datenschutzanforderungen wie Protokollierungs- und Kennzeichnungspflichten.

Im Ergebnis ist die Datenschutzkontrolle einer Verarbeitung ohne eine Rechtmäßigkeitsprüfung der Maßnahme jedoch nicht denkbar.²⁹¹

²⁸⁹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17.

²⁹⁰ Bund-Länder-AG zu BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17, Anlage 3, Institutionelle Anforderungen an unabhängige Kontrolle, S. 11.

²⁹¹ Dessen ungeachtet können Kontrollen – etwa von automatisierten Dateisystemen – auch losgelöst von einzelnen Verarbeitungen erfolgen. Insoweit ist dann nicht die Rechtmäßigkeit einzelner Maßnahmen zu prüfen, sondern lediglich die strukturelle Rechtmäßigkeit des Systems.

d. Spezielle Einbindung der Datenschutzbeauftragten

Viele Fachgesetze enthalten zusätzlich Regelungen, wonach die Datenschutzbeauftragten vor dem Erlass von Dateianordnungen angehört werden müssen.²⁹² Durch Dateianordnungen sollen bereits bei der Errichtung automatisierter Dateien „verfahrenstechnische und verfahrensrechtliche Schranken“ vorgesehen werden, um zu verhindern, dass die Daten „über das für die Aufgabenerfüllung erforderliche Maß“ verwendet werden.²⁹³ Die Anhörung gibt den Datenschutzbeauftragten die Möglichkeit, auf problematische Aspekte hinzuweisen und „sich einen fortlaufenden Überblick über die Dateienlandschaft der Nachrichtendienste zu verschaffen“.²⁹⁴

Gemäß mehreren Fachgesetzen können sich Betroffene an die Datenschutzbeauftragten wenden, wenn sie sich gegen eine aus ihrer Sicht unzureichende Auskunft des Nachrichtendienstes zur Wehr setzen wollen.²⁹⁵ Zudem enthalten manche Gesetze ein Jedermann-Beschwerderecht.²⁹⁶ Damit wird Betroffenen ermöglicht, sich an die Datenschutzbeauftragten zu wenden, wenn sie der Ansicht sind, bei der Verarbeitung personenbezogener Daten durch die Nachrichtendienste in ihren Rechten verletzt worden zu sein.

Zudem können einige Parlamentarischen Kontrollgremien²⁹⁷ oder G 10-Kommissionen²⁹⁸ die Datenschutzbeauftragten damit beauftragen, in ihrem Auftrag die Rechtmäßigkeit bestimmter Datenverarbeitungen zu kontrollieren.

²⁹² § 14 Abs. 1 S. 2 [BVerfSchG](#); § 8 MADG; § 8 BNDG; § 14 Abs. 2 [VerfSchG MV](#); § 27 Abs. 1 S. 2 [HVSg](#); § 23a Abs. 1 S. 3 [HmbVerfSchG](#); § 19 Abs. 2 S. 2 [SächsVSG](#); § 15 Abs. 2 [BremVerfSchG](#); § 16 Abs. 2 [ThürVerfSchG](#); Art. 22 Abs. 1 S. 1 [BayVSG](#); § 13 Abs. 3 S. 3 [BWLVSg](#); § 14 Abs. 1 S. 2 [SVerfSchG](#); Erlass „im Benehmen mit der oder dem“ LfDI; § 16 Abs. 1 [VSG Bln](#); § 15 S. 1 [LVerfSchG SH](#).

²⁹³ [Br-Drs. 11/4306](#), Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 6.4.1989, S. 62; Schenke/Graulich/Ruthig/Mallmann, § 14 BVerfSchG Rn. 2.

²⁹⁴ *Sosna*, GSZ 2022, 245, 248.

²⁹⁵ § 15 Abs. 4 S. 3 [BVerfSchG](#); § 13 Abs. 3 S. 3 [BWLVSg](#); § 26 Abs. 3 S. 2 [HVSg](#); § 14 Abs. 4 S. 3 [VSG NRW](#); § 23 Abs. 4 S. 3 [HmbVerfSchG](#); § 30 Abs. 4 S. 4 [NVerfSchG](#), beachte auch § 28 Abs. 1 [NVerfSchG](#); § 20 Abs. 6 S. 3 [SächsVSG](#); § 16 Abs. 3 S. 4 [BremVerfSchG](#); § 17 Abs. 4 S. 3 [ThürVerfSchG](#); § 14 Abs. 4 S. 3 [VerfSchG-LSA](#); § 12 Abs. 3 S. 2 [BbgVerfSchG](#); § 26 Abs. 4 S. 2 [VerfSchG MV](#); Art. 23 Abs. 3 S. 2 [BayVSG](#); § 13 Abs. 3 S. 3 [BWLVSg](#); § 29 Abs. 3 S. 3 [LVerfSchG RP](#); § 21 Abs. 3 S. 3 [SVerfSchG](#); § 31 Abs. 4 S. 1 [VSG Bln](#); § 25 Abs. 4 [LVerfSchG SH](#).

²⁹⁶ § 28 Abs. 1 BVerfSchG; § 15 Abs. 1 [VSG NRW](#); § 39 Abs. 2 S. 1 [SächsVSG](#); § 32a Abs. 1 [VSG Bln](#).

²⁹⁷ § 39 [NVerfSchG](#); § 28 [VerfSchG-LSA](#); § 29 Abs. 2 S. 2 [VerfSchG MV](#); Stellungnahmerecht gem. § 16d Abs. 4 [BWLVSg](#); § 25 Abs. 1 [SVerfSchG](#); § 4 Abs. 6 [VerfSchutzKG HE](#); § 25 Abs. 5 [VSG NRW](#); § 25 Abs. 7 [BbgVerfSchG](#); § 18 Abs. 7 [BbgDSG](#); *Michel*, GSZ 2021, 197, 202.

²⁹⁸ § 15 Abs. 5 G 10; § 30 Abs. 1 S. 2 [LVerfSchG RP](#); § 6 Abs. 2 [G10AG RP](#); § 30 Abs. 5 S. 4 [VSG NRW](#); § 2 Abs. 4 S. 3 [AG G 10 BW](#); § 4 Abs. 1 S. 4 [HAGG10](#); § 3 Abs. 6 S. 4 [G10DGSL](#); § 3 Abs. 1 S. 7 [AG G10 Bremen](#); § 26a Abs. 1 S. 2 [LVerfSchG SH](#); § 15 Abs. 5 G 10; § 3 Abs. 2 [AG G 10 MV](#); § 3 Abs. 1 S. 6 [G10AGBbg](#); § 2 Abs. 2 S. 3, 4 [AG G10 Bln](#); § 2 Abs. 2 S. 4 [Sächs AGG10](#); § 5 Abs. 3 [AG G 10-LSA](#); § 4 Abs. 3 [Nds AG G 10](#); § 3 Abs. 3 [AGG10 TH](#).

2. Unproblematische rechtskonforme Aspekte

Die einfach-rechtliche Ausgestaltung der Datenschutzkontrolle der Nachrichtendienste ist in vielerlei Hinsicht mit den höherrangigen Vorgaben vereinbar.

a. Kontrolleur

Dies betrifft zunächst den mit der Datenschutzkontrolle beauftragten Kontrolleur. Da der Gesetzgeber bei der Frage, wen er mit der Kontrolle betraut, einen Beurteilungsspielraum hat, bestehen keine verfassungsrechtlichen Einwände gegen die Beauftragung der Datenschutzbeauftragten.

b. Zeitpunkt

Bei der Kontrolle durch die Datenschutzbeauftragten handelt es sich in verfassungs- und konventionskonformer Weise um Kontrollen während der Durchführung bzw. ex post-Kontrollen.

c. Distanz

Beim BfDI und den Landesdatenschutzbeauftragten handelt es sich um unabhängige, weisungsfreie Behörden²⁹⁹, sodass die höherrangigen Vorgaben an die notwendige Distanz zwischen Kontrolleur und Kontrolliertem gewahrt werden.

d. Initiative

Verfassungsrechtlich sprechen bei der Datenschutzkontrolle die besseren Argumente für ein Kontrollinitiativrecht des Datenschutzkontrolleurs.³⁰⁰ Explizite Formulierungen, wonach der Datenschutzkontrolleur auf seine Initiative hin kontrolliert, enthalten die Fachgesetze allerdings nicht. Aber auch das Gegenteil, nämlich ein Kontrollinitiativrecht des Kontrollierten, ist nicht normiert.

Dennoch ist wegen der notwendigen Wirksamkeit der Kontrollen von einem Initiativrecht der Datenschutzbeauftragten auszugehen.³⁰¹ Soweit die Kontrolle der Nachrichtendienste in den Fachgesetzen explizit angeordnet wird, spricht auch die aktive

²⁹⁹ § 10 BDSG; § 8 Abs. 2 [HDSIG](#); § 21 Abs. 1, 2 [DSG BW](#); § 14 Abs. 1 [DSG RP](#); § 25 Abs. 2 [DSG NRW](#); u.a. Umkehrschluss aus § 21 Abs. 6 [HmbDSG](#); § 18 Abs. 1 [NDSG](#); § 17 [BremDSGVOAG](#); u.a. Umkehrschluss aus § 4 Abs. 6 [ThürDSG](#); § 22 Abs. 1 [DSAG-LSA](#); § 10 Abs. 2 [Bln DSG](#); § 16 Abs. 1 [BbgDSG](#); § 17 Abs. 1, § 21 Nr. 15 [LDSG SH](#); § 16 Abs. 4 [SDSG](#); Art. 18 Abs. 1 [BayDSG](#), Art. 51 DSGVO; § 17 25 [DSG MV](#); nicht normiert im [SächsDSG](#).

³⁰⁰ Vgl. [Teil 2 A. III. 1. a. ff.](#), [Teil 2 A. III. 1. b. ff.](#)

³⁰¹ Vgl. [Teil 2 A. III. 1. a. ff.](#), [Teil 2 A. III. 1. b. ff.](#)

Formulierung für das Initiativrecht des Kontrollleurs (z.B. „Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert (...)“).³⁰² Demgegenüber wird eine andere Aufgabe häufig im Passiv formuliert: So ist der Datenschutzbeauftragte anzuhören, bevor der Nachrichtendienst eine Dateianordnung zur Errichtung automatisierter Dateien erlässt³⁰³. Weil der Datenschutzkontrolleur darauf angewiesen ist, vom Nachrichtendienst zunächst über die Dateianordnung informiert zu werden, geht hier die Initiative vom Kontrollierten aus.

Darüber hinaus werden die Datenschutzbeauftragten teilweise auch auf Initiative Betroffener hin tätig, die sich gegen eine Auskunftsverweigerung oder Datenverarbeitung der Nachrichtendienste wehren.³⁰⁴ Außerdem werden sie vereinzelt von der G 10-Kommission beauftragt.³⁰⁵

3. Modalität

Die Datenschutzkontrolle durch den BfDI erfolgt stichprobenartig, das Bundesverfassungsgericht fordert ein „regelmäßiges“ Intervall von maximal zwei Jahren zwischen den Stichprobenkontrollen.³⁰⁶ Diese Zeitspanne von nicht mehr als zwei Jahren zwischen zwei Datenschutzkontrollen ist vor dem Hintergrund der übrigen Vorgaben des Bundesverfassungsgerichts nicht überzeugend. Vermutlich hat das Gericht diesen Zeitraum aus Rücksicht auf die unterausgestatteten Datenschutzbehörden weit bemessen. Der vom Bundesverfassungsgericht geforderte Kontrollgesamtüberblick kann jedoch bei einem Kontrollintervall von zwei Jahren nicht verwirklicht werden. Deshalb müssen Kontrollen häufiger erfolgen.³⁰⁷

Teilweise haben sich die Gesetzgeber an der Rechtsprechung orientiert und ein Mindest-Kontrollintervall von zwei Jahren normiert.³⁰⁸ Überwiegend enthalten die Gesetze jedoch weder genaue Zeitangaben noch allgemeinere Vorgaben, wie etwa eine Formulierung, wonach „in regelmäßigen Abständen“ zu kontrollieren ist.

³⁰² U.a. § 28 Abs. 2 BVerfSchG.

³⁰³ Vgl. [Teil 3 D. II. 1. d.](#)

³⁰⁴ § 28 Abs. 1 BVerfSchG (§ 63 BNDG, § 13 a MADG, § 28 Abs. 1 BVerfSchG); § 18 Nr. 1 [BWLVSchG](#), § 25 Abs. 3 [DSG BW](#); § 15 Abs. 1 [VSG NRW](#); § 23b Abs. 1 [HmbVerfSchG](#); § 33a Abs. 1 S. 3 [NVerfSchG](#), § 57 Abs. 2 Nr. 6 [NDStG](#); § 18 Abs. 2 [SächsVerfSchG](#); § 32a Abs. 1 [VSG Bln](#); § 15 Abs. 1 Nr. 1 [HVSG](#), § 13 Abs. 2 S. 1 Nr. 6 [HDSIG](#); § 36 [ThürVerfSchG](#), § 8 Abs. 1 [ThürDSG](#); § 30 [VerfSchG-LSA](#), § 19 [DSG-LSA](#) in der Fassung der Bekanntmachung vom 13. Januar 2016.

³⁰⁵ [Teil 3 B. X. 2. e.](#)

³⁰⁶ Vgl. [Teil 2 A. III. 1. a. ee](#)), BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 217; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 141.

³⁰⁷ Vgl. [Teil 2 A. IV. 2. b. cc](#)).

³⁰⁸ § 17 Abs. 1 [BWLVSchG](#); § 33a Abs. 1 S. 2 [NVerfSchG](#); Art. 32 Abs. 2 [BayVSG](#).

Weil die Datenschutzkontrolle für die Verhältnismäßigkeit der Eingriffe von entscheidender Bedeutung ist, sollten die Vorgaben des Bundesverfassungsgerichts gesetzlich abgebildet werden, anstatt die Entscheidung über die (Mindest-)Anzahl der Stichprobenkontrollen den Datenschutzbehörden zu überlassen.

Soweit die Kontrollen seltener als alle zwei Jahre stattfinden, ist diese Praxis verfassungswidrig.

4. Ressourcen

Nach der Rechtsprechung des Bundesverfassungsgerichts sind die Datenschutzaufsichtsbehörden unter anderem personell so auszustatten, dass ihnen regelmäßige Kontrollen möglich sind.³⁰⁹ Ab wann eine ausreichende personelle Ausstattung bejaht werden kann, liegt im Beurteilungsspielraum des Gesetzgebers. Dabei darf jedoch eine (pauschal nicht definierbare) personelle Untergrenze, bei der regelmäßige Kontrollen nicht mehr gewährleistet werden können, nicht unterschritten werden.

Von den der Öffentlichkeit zur Verfügung gestellten Organigrammen der Datenschutzbeauftragten legen nur die aus Hessen und Brandenburg den Stellenanteil einzelner Bereiche offen, in den übrigen Organigrammen wird lediglich der Referatsleiter genannt. Im Übrigen stammen die Informationen über die Ressourcen aus den Antworten der Datenschutzbehörden auf die Anfragen der Autorin. Da die relevanten Informationen für Hessen und Brandenburg online recherchierbar sind, wurden die übrigen 15 Datenschutzbehörden angefragt. Neun von ihnen haben geantwortet.³¹⁰

a. Stellenanteile

Dementsprechend liegen Daten von elf Kontrolleuren vor.

aa) Bund

Für die Datenschutzkontrolle der Nachrichtendienste steht dem BfDI mit insgesamt 29 vorgesehenen Stellen in allen Laufbahnen im Vergleich mit den Ländern das meiste Personal zur Verfügung. Die beiden für die Nachrichtendienste zuständigen Referate kontrollieren jedoch – anders als ihre Äquivalente in den Ländern – nicht nur den Verfassungsschutz, sondern auch den BND, den MAD, die Zentrale Stelle für Informationstechnik im Sicherheitsbereich und das Militärische Nachrichtenwesen. Dennoch ist anzunehmen, dass bei 29 Vollzeitstellen regelmäßige Kontrollen möglich sind.

³⁰⁹ Vgl. [Teil 2 A. III. 1. a. ii\)](#), BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 217; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 141.

³¹⁰ BfDI, BlnBDI, LfDI Sachsen-Anhalt, ULD Schleswig-Holstein, LDI NRW, UDZ Saarland, Sächsische Datenschutz und Transparenzbeauftragte, LfDI Bremen, HmbBfDI.

bb) Länder

Für die Kontrolle der Landesämter für Verfassungsschutz ist bei den Landesdaten-schutzbehörden in der Regel weniger als eine Stelle vorgesehen. Die Beamten eines Re-ferats sind häufig zugleich für die Datenschutzkontrolle weiterer Sicherheitsbehörden und sogar der Justiz zuständig.

So sind in Hessen im Referat 1.1 mit der Zuständigkeit für „Justiz, Polizei, Strafvoll-zug, Rechtsanwälte, Notare und deren Kammern, Verfassungsschutz, gesetzl. Prüf-pflichten, Videoüberwachung im Polizei- und Justizbereich, Vertretung in bereichs-spezifischen EU-Gremien“ insgesamt vier Personen angestellt.³¹¹ In Anbetracht der Größe der hessischen Justiz und Polizei, deren Mitarbeiterzahl sich insgesamt im fünf-stelligen Bereich bewegt, wird vermutlich für die Datenschutzkontrolle des vergleichs-weise kleinen LfV mit 381 Planstellen (Stand 2022³¹²) maximal eine, vermutlich sogar nur eine halbe Stelle eingeplant sein.

Wie in Hessen sind auch in NRW insgesamt nur vier Personen im Referat 2 zur Kontrolle von Polizei, Justiz und Verfassungsschutz angestellt. Wie viele Vollzeitäqui-valente von diesen zwei Stellen auf die Kontrolle des Verfassungsschutzes entfallen, lässt sich nach Angaben der Datenschutzbehörde nicht beziffern, weil die Kontrollaufgaben „über das Jahr nicht gleichmäßig anfallen“.³¹³

In vier weiteren Bundesländern sind für die Kontrolle der Gefahrenabwehrbehör-den, der Justiz und des Verfassungsschutzes insgesamt jeweils zwei Stellen vorgese-hen.³¹⁴ Beim Datenschutzbeauftragten in Hamburg werde der Kontrolle des Verfas-sungsschutzes eine Priorisierung eingeräumt, weshalb beide Referenten dieser Aufgabe jeweils circa 20 Prozent ihres Vollzeitäquivalents widmen.³¹⁵ Beim Datenschutzbeauf-tragten in Schleswig-Holstein nimmt die Kontrolle des Verfassungsschutzes 10 bis ma-ximal 20 Prozent eines Vollzeitäquivalents ein.³¹⁶

Im Übrigen gibt es Länder, in denen lediglich eine Stelle eingeplant ist. So ist im Saarland für die Datenschutzkontrolle nur eine Stelle vorgesehen, wobei die daten-schutzrechtliche Kontrolle der Polizei etwa 70- 80 Prozent einnehme und die restlichen

³¹¹ <https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-05/Organi-gramm%20vom%201.4.2023.pdf> (abgerufen am 31.8.2024).

³¹² https://verfassungsschutz.hessen.de/sites/verfassungsschutz.hessen.de/files/2022-12/lfv_be-richt21_barrfrei_v2_0.pdf, S. 22 (abgerufen am 15.4.2024).

³¹³ Antwort des ständigen Vertreters des LfDI NRW per E-Mail v. 6.4.2023.

³¹⁴ Antwort aus dem zuständigen Referat des Landesbeauftragten für den Datenschutz des Landes Sachsen-Anhalt per E-Mail v. 6.4.2023, vorgesehen sei ein Referent und ein Sachbearbeiter; Antwort aus dem zuständigen Referat der Sächsischen Datenschutz- und Transparenzbeauftragten v. 5.4.2023; Ant-wort aus dem zuständigen Referat des HmbBfDI per E-Mail v. 11.4.2023, Antwort der Datenschutzbe-auftragten v. Schleswig-Holstein, Marit Hansen, v. 6.4.2023.

³¹⁵ Antwort aus dem zuständigen Referat des HmbBfDI per E-Mail v. 11.4.2023.

³¹⁶ Antwort der Datenschutzbeauftragten v. Schleswig-Holstein, Marit Hansen, v. 6.4.2023.

20- 25-Prozent auf Verfassungsschutz und Justiz entfallen würden.³¹⁷ In Brandenburg ist eine Person für die Kontrolle des Verfassungsschutzes zuständig, die darüber hinaus auch den Strafvollzug kontrolliert, Gruppenleiterin von acht Mitarbeitern ist und die Funktion der stellvertretenden Pressesprecherin wahrnimmt.³¹⁸ Auch der zuständige Mitarbeiter beim Berliner Datenschutzbeauftragten hat weitere Aufgaben.³¹⁹

In Bremen gibt es laut Aussagen der Behörde keinen fest eingeplanten Stellenanteil weder für den Verfassungsschutz noch für die Kontrolle von Sicherheitsbehörden und Justiz an sich.³²⁰

b. Ressourcenmangel in den Ländern

Im Ergebnis gibt es unter den zehn Landesdatenschutzbehörden, über die Daten vorliegen, nicht eine, in der ein Referent sich der Kontrolle des Verfassungsschutzes in Vollzeit widmen kann. Das liegt daran, dass die Datenschutzkontrolle im Bereich der gesamten inneren Sicherheit und Justiz durch ein Referat mit ein bis vier Stellen erfolgen muss. Dabei wird der Schwerpunkt stets auf der Kontrolle von Datenverarbeitungen der Polizei liegen müssen, weil die Polizeien personenbezogene Daten von deutlich mehr Personen verarbeiten.³²¹

Bei den größeren Landesämtern für Verfassungsschutz wie denjenigen in Hessen und NRW ist allein wegen der Mitarbeiterzahl ([381 Planstellen in Hessen](#), [556 in NRW](#)³²²) von einem höheren Aufkommen an nachrichtendienstlichen Datenverarbeitungen auszugehen. Trotzdem ist auch für die Kontrolle dieser Behörden kein Mitarbeiter in Vollzeit oder zumindest mit einer halben Stelle angestellt.

Insgesamt ist fraglich, ob regelmäßige Kontrollen sichergestellt werden können, wenn dafür weniger als eine halbe Stelle vorgesehen ist und von dem Mitarbeiter zudem häufig noch weitere Aufgaben zu bearbeiten sind. Hinzu kommt, dass es sich bei den Stichprobenkontrollen nicht um die einzige Aufgabe der Datenschutzbehörde im Bereich „Verfassungsschutz“ handelt: Denn die Datenschutzbeauftragten müssen zusätzlich Dateianordnungen prüfen, auf Betroffenenbeschwerden reagieren und den Gesetzgeber beraten.

³¹⁷ Antwort aus dem Unabhängigen Datenschutzzentrum des Saarlands v. 6.4.2023, in der darauf hingewiesen wird, dass sie eine Personalaufstockung fordern.

³¹⁸ https://www.lda.brandenburg.de/sixcms/media.php/9/Organigramm_240214.4439473.pdf (abgerufen am 31.8.2024).

³¹⁹ Antwort des Pressesprechers des BlnBDI, v. 31.5.2023.

³²⁰ Antwort aus der Verwaltung der LfDI Bremen v. 1.6.2023.

³²¹ So auch die Antwort der Datenschutzbeauftragten v. Schleswig-Holstein, Marit Hansen, v. 6.4.2023.

³²² https://www.im.nrw/system/files/media/document/file/verfassungsschutzbericht_nrw_2022.pdf, (abgerufen am 31.8.2024), https://verfassungsschutz.hessen.de/sites/verfassungsschutz.hessen.de/files/2022-12/lfv_bericht21_barrierefrei_v2_0.pdf (abgerufen am 31.8.2024).

Abschließend zeigen die Ergebnisse der Recherche, dass bei den Landesdatenschutzbeauftragten keine ausreichenden Ressourcen für die Kontrolle der Nachrichtendienste vorgesehen sind. Bei einer so geringen Stellenausstattung sind „regelmäßige“ Stichprobenkontrollen nicht umsetzbar.

5. Kontrollmittel zur Informationsgewinnung

Die Datenschutzbeauftragten verfügen über diverse Kontrollmittel zur Informationsgewinnung.

a. Unterstützungspflicht

Zunächst verpflichten viele Fachgesetze die Nachrichtendienste dazu, den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen.³²³

b. Akteneinsichts- und Auskunftsrecht

Die Datenschutzbeauftragten haben im Rahmen ihres Kontrollauftrags ein Recht auf Auskunft zu ihren Fragen und auf Einsicht in alle Unterlagen sowie alle gespeicherten Daten und Datenverarbeitungsprogramme.³²⁴ In Bayern besteht nur ein Recht zur Anforderungen von Unterlagen zur Einsicht, aber kein Recht zur Einsichtnahme in Datenverarbeitungsprogramme.³²⁵ In Brandenburg kann die Einsicht sogar „elektronisch“ erfolgen (§ 27 Abs. 1 Nr. 1 BbgVerfSchG i. V. m. § 21 Abs. 1 S. 3 BbgDSG). In Bremen kann die Datenschutzbehörde darüber hinaus „nach festgelegten Vorgaben strukturierte Auswertungen aus automatisierten Informationssystemen verlangen, soweit dies

³²³ § 28 Abs. 3 S. 1 [BVerfSchG](#) (§ 63 BNDG, § 13a MADG, § 28 Abs. 3 S. 1 BVerfSchG); § 15 Abs. 1 Nr. 1 [HVSG](#), § 14 Abs. 4 S. 1 [HDSIG](#); § 18 Nr. 1 [BWLVSIG](#), § 26 Abs. 1 S. 1 [DSG BW](#); § 15 Abs. 3 S. 1 [VSG NRW](#); § 23b Abs. 3 S. 1 [HmbVerfSchG](#); § 33a Abs. 2 S. 1 [NVerfSchG](#); § 31 [BremVerfSchG](#), § 21 Abs. 5 S. 2 [BremDSGVOAG](#); § 39 Abs. 4 S. 1 [SächsVSG](#); § 36 [ThürVerfSchG](#), § 7 Abs. 5 S. 1 [ThürDSG](#); § 32a Abs. 3 S. 1 [VSG Bln](#); § 3 Abs. 1, § 20 Abs. 4 S. 1 [SDSG](#); § 30 [VerfSchG-LSA](#), § 23 Abs. 1 S. 1 [DSG-LSA](#) in der Fassung der Bekanntmachung vom 13. Januar 2016; § 27 Abs. 1 Nr. 1 [BbgVerfSchG](#), § 21 Abs. 1 S. 1 [BbgDSG](#); Art. 32 Abs. 2 [BayVSG](#), Art. 16 Abs. 1 S. 1 [BayDSG](#); § 2 Abs. 7 Nr. 1, § 18 Abs. 1 S. 1 [LDSG SH](#).

³²⁴ § 28 Abs. 3 S. 2 BVerfSchG (§ 63 BNDG, § 13a MADG, § 28 Abs. 3 S. 2 BVerfSchG); § 15 Abs. 1 Nr. 1 [HVSG](#), § 14 Abs. 4 S. 2 Nr. 1, 2 [HDSIG](#); § 18 Nr. 1 [BWLVSIG](#), § 26 Abs. 1 S. 2 Nr. 1 [DSG BW](#); § 30 Abs. 2 S. 2 [LVerfSchG RP](#); § 15 Abs. 3 S. 2 Nr. 1 [VSG NRW](#); § 23b Abs. 3 S. 2 Nr. 1 [HmbVerfSchG](#); § 33a Abs. 2 S. 2 Nr. 1 [NVerfSchG](#); § 31 [BremVerfSchG](#), § 21 Abs. 5 S. 3 Nr. 1 [BremDSGVOAG](#); § 39 Abs. 4 S. 2 [SächsVSG](#); § 32a Abs. 3 S. 2 Nr. 1 [VSG Bln](#); § 3 Abs. 1, § 20 Abs. 4 S. 2 Nr. 1 [SDSG](#); § 30 [VerfSchG-LSA](#), § 23 Abs. 1 S. 2 Nr. 1 [DSG-LSA](#) in der Fassung der Bekanntmachung vom 13. Januar 2016; § 27 Abs. 1 Nr. 1 [BbgVerfSchG](#), § 21 Abs. 1 S. 2 Nr. 1 [BbgDSG](#); § 2 Abs. 7 Nr. 1, § 18 Abs. 1 S. 2 Nr. 1 [LDSG SH](#).

³²⁵ Art. 32 Abs. 2 [BayVSG](#), Art. 16 Abs. 1 S. 2 [BayDSG](#).

die bei den jeweiligen öffentlichen Stellen bestehenden technischen Möglichkeiten zu lassen“.³²⁶ In Thüringen besteht eine „Pflicht zur Information“.³²⁷

c. Zutrittsrecht

Überwiegend ist den Datenschutzbeauftragten jederzeit Zutritt in alle Diensträume zu gewähren.³²⁸ In Sachsen muss der Datenschutzbeauftragte den Verfassungsschutz vor Beginn einer Kontrolle informieren (§ 39 Abs. 4 S. 3 SächsVSG). Teilweise ist die Formulierung abgeschwächt, sodass zwar der Zugang zu den Diensträumen verlangt werden kann, allerdings nicht jederzeit.³²⁹

d. Beauftragung von Mitarbeitern

Überwiegend erstrecken sich die Unterstützungspflichten und die weiteren Kontrollmittel auf durch den Datenschutzbeauftragten (schriftlich) besonders Beauftragte.³³⁰ Teilweise wird in diesem Zusammenhang vorausgesetzt, dass sich die Beauftragten einer (erweiterten) Sicherheitsüberprüfung unterzogen haben.³³¹

e. Keine vergleichbaren Kontrollmittel in Mecklenburg-Vorpommern

In Mecklenburg-Vorpommern stehen dem Landesdatenschutzbeauftragten aufgrund der widersprüchlichen Rechtslage derzeit einfach-rechtlich keine der oben genannten Befugnisse zu.

³²⁶ § 31 [BremVerfSchG](#), § 21 Abs. 5 S. 3 Nr. 2 [BremDSGVOAG](#).

³²⁷ Umkehrschluss aus § 7 Abs. 5 S. 1 [ThürDSG](#).

³²⁸ § 28 Abs. 3 S. 2 BVerfSchG (§ 63 BNDG, § 13a MADG, § 28 Abs. 3 S. 2 BVerfSchG); § 18 Nr. 1 [BWLVS](#), § 26 Abs. 1 S. 2 Nr. 2 [DSG BW](#); § 15 Abs. 3 S. 2 Nr. 2 [VSG NRW](#); § 23b Abs. 3 S. 2 Nr. 2 [HmbVerfSchG](#); § 33a Abs. 2 S. 2 Nr. 2 [NVerfSchG](#); § 31 [BremVerfSchG](#), § 21 Abs. 5 S. 3 Nr. 3 [BremDSGVOAG](#); § 39 Abs. 4 S. 2 [SächsVSG](#); § 36 [ThürVerfSchG](#), § 7 Abs. 2 [ThürDSG](#); § 32a Abs. 3 S. 2 Nr. 2 [VSG Bln](#); § 3 Abs. 1, § 20 Abs. 4 S. 2 Nr. 2 [SDSG](#); § 30 [VerfSchG-LSA](#), § 23 Abs. 1 S. 2 Nr. 2 [DSG-LSA](#) in der Fassung der Bekanntmachung vom 13. Januar 2016; § 27 Abs. 1 Nr. 1 [BbgVerfSchG](#), § 21 Abs. 1 S. 2 Nr. 2 [BbgDSG](#).

³²⁹ § 15 Abs. 1 Nr. 1 [HVS](#), § 14 Abs. 4 S. 2 Nr. 3 [HDSIG](#); § 30 Abs. 2 S. 1 [LVerfSchG RP](#); Art. 32 Abs. 2 [BayVSG](#), Art. 16 Abs. 1 S. 3 [BayDSG](#); § 2 Abs. 7 Nr. 1, § 18 Abs. 1 S. 2 Nr. 2 [LDSG SH](#).

³³⁰ § 28 Abs. 3 S. 2 BVerfSchG (§ 63 BNDG, § 13a MADG, § 28 Abs. 3 S. 2 BVerfSchG); Umkehrschluss aus § 14 Abs. 5 S. 2 [HDSIG](#); § 17 Abs. 2 [BWLVS](#), hier ist auch ein leitender Beamter dazu berechtigt, für diese Aufgaben Mitarbeiter schriftlich zu beauftragen; § 30 Abs. 3 [LVerfSchG RP](#); § 15 Abs. 3 S. 1 [VSG NRW](#); § 23b Abs. 3 S. 1 [HmbVerfSchG](#); Umkehrschluss aus § 33a Abs. 2 S. 3 [NVerfSchG](#); § 39 Abs. 4 S. 1 [SächsVSG](#); § 36 [ThürVerfSchG](#), § 7 Abs. 5 S. 1 [ThürDSG](#); § 32a Abs. 3 S. 1 [VSG Bln](#); § 3 Abs. 1, § 20 Abs. 4 S. 1 [SDSG](#); § 30 [VerfSchG-LSA](#), § 23 Abs. 2 S. 1 [DSG-LSA](#) in der Fassung der Bekanntmachung vom 13. Januar 2016; § 27 Abs. 1 Nr. 1 [BbgVerfSchG](#), § 21 Abs. 1 S. 1 [BbgDSG](#); Art. 32 Abs. 2 [BayVSG](#), Art. 16 Abs. 2 S. 1 [BayDSG](#).

³³¹ § 30 Abs. 3 S. 1 [LVerfSchG RP](#); § 27 Abs. 1 Nr. 1 [BbgVerfSchG](#), § 21 Abs. 1 S. 1 [BbgDSG](#).

Außer dem Einsichtnahmerecht, das aus der Protokollierungspflicht zu Kontrollzwecken folgt, sind keine der genannten Befugnisse verfassungsrechtlich zwingend vorgegeben. Das Bundesverfassungsgericht fordert „wirksame Befugnisse“ und überlässt deren nähere Ausgestaltung dem Gesetzgeber. Deshalb kann der LfDI in Mecklenburg-Vorpommern zwar seine Zuständigkeit verfassungsrechtlich herleiten, mangels Konkretisierung durch das Bundesverfassungsgericht jedoch nicht die in den anderen Ländern vorgesehenen Befugnisse.

Das Kontrolldesign in Mecklenburg-Vorpommern ist verfassungswidrig, weil dem LfDI keine Befugnisse zustehen.

f. Weitreichende Ausnahmetatbestände

Die aufgezeigten Kontrollmittel zur Informationsgewinnung gelten jedoch in vielen Ländern und auf der Bundesebene nicht uneingeschränkt (dazu vertieft unter „7. Barrieren“)³³².

6. Kontrollerggebnisfolgen

Der Datenschutzkontrolleur muss mit „wirksamen“ Befugnissen ausgestattet sein.³³³ Welche Kontrollerggebnisfolgen „wirksam“ sind, hat der Gesetzgeber zu entscheiden (vgl. a., b.). Dabei darf jedoch eine Untergrenze nicht unterschritten werden, unterhalb der von einer Wirksamkeit der Kontrollfolge nicht mehr ausgegangen werden kann. Um diese Grenze näher zu bestimmen, wird auf das Erfahrungswissen der Kontrolleure zurückgegriffen (vgl. c.).

Jedenfalls in Teilen sind die nach einfachem Recht vorgesehenen Kontrollerggebnisfolgen nicht unionsrechtskonform (vgl. d.).

a. Kontrollerggebnisfolgen de lege lata

Die Kontrollergebnisse des BfDI gegenüber den Nachrichtendiensten des Bundes richten sich nach § 16 Abs. 2 BDSG: Soweit der BfDI Verstöße gegen den Datenschutz oder Mängel bei der Verarbeitung personenbezogener Daten feststellt, beanstandet er diese gegenüber der zuständigen obersten Bundesbehörde und fordert sie innerhalb einer von ihm bestimmten Frist zur Stellungnahme auf. Bei unerheblichen oder zwischenzeitlich beseitigten Mängeln kann der BfDI auf eine Beanstandung verzichten. In der

³³² Vgl. [Teil 3 D. II. 7. b.](#)

³³³ Vgl. [Teil 2 A. III. 1. a. hh](#); BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 214 f.; BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 141; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290.

Stellungnahme sollen die Maßnahmen dargestellt werden, die aufgrund der Beanstandung getroffen worden sind. Zusätzlich zur Beanstandung kann der BfDI bezüglich beabsichtigter Datenverarbeitungen eine Warnung aussprechen. Die Beanstandung hat keine Regelungswirkung, weshalb sie kein Mittel zur Rechtsdurchsetzung ist, sondern allein als politisches Druckmittel dient.³³⁴ Durch sie wird ein „eingehendes Prüfverfahren“ ausgelöst, an dessen Ende die Aufsichtsbehörde, gegenüber der die Beanstandung ausgesprochen wurde, entweder Maßnahmen ergreifen wird, um der Beanstandung abzuhelpen oder die Beanstandung inhaltlich zurückweist.³³⁵

In den Bundesländern gibt es unterschiedliche Regelungsmodelle. In Mecklenburg-Vorpommern sind als Folge der widersprüchlichen Rechtslage *de lege lata* keine Kontrollerggebnisfolgen vorgesehen, weshalb das Kontrolldesign verfassungswidrig ist. Manche Landesverfassungsschutzgesetze enthalten selbst dem § 16 Abs. 2 BDSG vergleichbare Normen³³⁶; andere verweisen entweder auf § 16 Abs. 2 BDSG³³⁷ oder auf inhaltlich identische Normen im Landesdatenschutzgesetz³³⁸.

Teilweise sind in den Landesgesetzen darüber hinaus weitergehende Befugnisse etabliert worden. So kann der Datenschutzbeauftragte in manchen Ländern zusätzlich das PKGr über den Verstoß unterrichten (§ 33a Abs. 3 S. 2 Nr. 2 NVerfSchG, § 38 VSG Bln i. V. m. § 13 Abs. 2, 3 BlnDSG).

Manche Landesdatenschutzbeauftragten können fordern, dass innerhalb einer bestimmten Frist „geeignete Maßnahmen“ zu treffen sind, wenn die Beanstandung erfolglos geblieben ist; falls auch diese „geeigneten Maßnahmen“ nach Fristablauf nicht ergriffen wurden, können sie den Landtag und die Landesregierung „verständigen“.³³⁹

Vereinzelte verweisen die Landesgesetze sogar auf Art. 58 Abs. 2 DSGVO. Die Verweise sind in ihrer Reichweite jedoch nicht identisch: Der Verweis in § 27 Abs. 2 Bbg-VerfSchG ist auf Art. 58 Abs. lit.a) und b) DSGVO, also auf die Warnung und die Verwarnung, begrenzt. Dabei ist eine Verwarnung mit der Beanstandung vergleichbar.³⁴⁰

³³⁴ Schenke/Graulich/Ruthig/Ruthig, § 69 BKAG Rn. 12.

³³⁵ Schulze/Bange, ZD 2019, 199, 200 f.

³³⁶ § 15 Abs. 5 VSG NRW; § 33a Abs. 3 NVerfSchG; § 3 Abs. 1, § 20 Abs. 2 SDSG (der jedoch weit darüber hinausgeht); § 39 Abs. 3 SächsVSG.

³³⁷ § 18 Nr. 2 BWLVSG; § 16 Abs. 2 BDSG; § 23c HmbVerfSchG; § 16 Abs. 2 BDSG; § 2 Abs. 7 Nr. 2 LDSG SH; § 16 Abs. 2 BDSG, wobei hier die Rechtsgrundlage nicht ganz eindeutig ist, da § 2 Abs. 7 Nr. 1 die Anwendbarkeit von § 17 LDSG SH gerade nicht ausschließt, in dessen Absatz 2 auf die Art. 58 Abs. 2 lit.c-g DSGVO verwiesen wird. Weil § 2 Abs. 7 Nr. 2 LDSG SH explizit auf § 16 Abs. 2 BDSG verweist, während die Geltung von § 17 Abs. 2 LDSG SH lediglich nicht ausgeschlossen ist, erscheint es naheliegender, darauf abzustellen.

³³⁸ § 15 Nr. 1 HVSG; § 14 Abs. 2 HDSIG; § 39 LVerfSchG RP; § 42 Abs. 1 DSG RP; § 38 VSG Bln; § 13 Abs. 2 BlnDSG; § 36 ThürVerfSchG; § 7 Abs. 6 ThürDSG; Art. 32 Abs. 2 BayVSG; Art. 16 Abs. 4 BayDSG; § 30 VerfSchG-LSA; § 24 DSG-LSA in der Fassung der Bekanntmachung vom 13. Januar 2016.

³³⁹ § 36 ThürVerfSchG; § 7 Abs. 6 S. 6 ThürDSG; Art. 32 Abs. 2 BayVSG; Art. 16 Abs. 4 S. 4 BayDSG.

³⁴⁰ Wolff/Brink/Eichler/Matzke, Art. 58 DSGVO Rn. 20.

Demgegenüber enthält § 3 Abs. 1, § 20 Abs. 2 SDStG keine Einschränkungen, er verweist vorbehaltlos auf Art. 58 Abs. 2 DSGVO³⁴¹. Gegenüber dem saarländischen Verfassungsschutz kann der LfDI daher sogar Anweisungen erteilen oder Beschränkungen und Verbote aussprechen. Auch § 21 Abs. 5 BremDSGVOAG, der auf der Grundlage von § 31 BremVerfSchG anwendbar ist, verweist vorbehaltlos auf Art. 58 DSGVO.

b. Grundsätzliche Option der Erwähnung im Tätigkeitsbericht

In der Literatur wird darauf hingewiesen, dass die Datenschutzbeauftragten „problematisch[e] Überwachungspraktiken“ in ihren Tätigkeitsberichten publizieren und so auf eine Veränderung drängen können.³⁴² Von dieser Möglichkeit können die Datenschutzbeauftragten jedoch nur in begrenztem Umfang Gebrauch machen, da die Arbeitsweisen der Nachrichtendienste aus Effektivitätsgründen grundsätzlich geheim bleiben müssen.³⁴³

Die Veröffentlichung im Tätigkeitsbericht ist zudem anders als die Beanstandung ein Mittel, um strukturelle Veränderungen anzustoßen; jedoch kein taugliches Mittel, um Datenschutzverletzungen im Einzelfall zu untersagen.

c. Beanstandung als wirksame Befugnis?

Auf der Bundesebene und in den meisten Bundesländern ist die Beanstandung das stärkste Instrument, das den Datenschutzbeauftragten zur Verfügung steht.³⁴⁴ Deshalb kommt es für die Beurteilung der Verfassungskonformität der Kontrollerggebnisfolgen nach geltendem Recht darauf an, ob es sich bei der Beanstandung um eine wirksame Befugnis handelt.

Eine Kontrollerggebnisfolge ist wirksam, wenn der rechtswidrige Zustand beendet wird.³⁴⁵

³⁴¹ Vgl. zu Art. 58 Abs. 2 DSGVO, [Teil 2 B. II. 2. b. cc](#)).

³⁴² *Kutscha*, NVwZ 2003, 1296, 1299 f.; auf die Tätigkeitsberichte hinweisend auch *Stoklas/Wendorf*, ZD-Aktuell 2016, 5345; *Bäumler*, RDV 1996, 163, 169; *Kornblum*, Rechtsschutz, S. 82.

³⁴³ *Gusy*, Richterliche Kontrolle, 67, 90; zu dieser Problematik auch der Neunte Tätigkeitsbericht des BfDI v. 28.1.1987, Bt-Drs. 10/6816, S. 63, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/09TB_86.pdf?__blob=publicationFile&v=8 (abgerufen am 31.8.2024); *Ruckerbauer*, Stärkung des Datenschutzbeauftragten, S. 4.

³⁴⁴ „Wichtigstes Instrument“, *Sosna*, GSZ 2022, 245, 247.

³⁴⁵ Vgl. [Teil 2 A. III. 1. a. hh](#)); *Geiger*, DVBl 1990, 748, 751.

Grundsätzlich ist die Beanstandung ein taugliches Mittel, um über ein Zusammenwirken³⁴⁶ von Datenschutzbeauftragten und der Aufsichtsbehörde datenschutzrechtliche Mängel abzustellen. Bei den Datenschutzkontrollen der Antiterrordatei beispielsweise führten Beanstandungen der Datenschutzbeauftragten zu einer Löschung oder Korrektur bestimmter Datensätze, teilweise konnten Beanstandungen sogar unterbleiben, weil die „sofortige Behebung“ bestimmter Mängel zugesagt worden war.³⁴⁷

Weil Beanstandungen jedoch nicht durchgesetzt werden können, stoßen sie zwangsläufig immer dann an ihre Grenzen, wenn die Aufsichtsbehörde die Auffassung der Datenschutzbeauftragten nicht teilt. Die Beanstandung bleibt dann wirkungslos. Der BfDI hat aus diesem Grund massive Zweifel an der Effektivität des Instruments der Beanstandung artikuliert.³⁴⁸

Ob die zuständige Aufsichtsbehörde den Nachrichtendienst in der Praxis anweist, den beanstandeten Zustand abzustellen, ist für die (Fach-)Öffentlichkeit nicht überprüfbar.³⁴⁹ Im Gegensatz dazu können die Datenschutzbeauftragten und deren Mitarbeiter beurteilen, ob und inwieweit aus ihren Beanstandungen Konsequenzen gezogen wurden. Im Urteil des Bundesverfassungsgerichts zur strategischen Auslands-Fernmeldeaufklärung wird die kritische Haltung des BfDI deutlich: Die verfassungsrechtlichen Kontrollvorgaben würden nur „unzureichend“ umgesetzt, es fehle an Sanktionsmöglichkeiten. Zudem seien Beanstandungen des BfDI ignoriert worden und schließlich folgenlos geblieben, weil eine Veröffentlichung des Vorgangs dem BfDI nicht möglich ist. Die objektive und unabhängige Kontrolle sei „insgesamt unzureichend“ und „nicht dazu geeignet, den aufgrund der Geheimhaltung der Maßnahmen in Ermangelung von Benachrichtigungspflichten faktisch fehlenden Rechtsschutz zu ersetzen.“³⁵⁰

Die Referatsleiterin für die Kontrolle unter anderem des BfV beim BfDI, Sosna, schildert, dass die zuständige Fachaufsichtsbehörde den Nachrichtendienst grundsätzlich auch gegen dessen Willen dazu „anhalten“ könne, festgestellte Verstöße zu beenden. In der Praxis sei jedoch feststellbar, „dass die Fachaufsicht häufig die Rechtsauffassung des verantwortlichen Nachrichtendienstes teilt und keine Abhilfemaßnahmen

³⁴⁶ *Schulze/Bange*, ZD 2019, 199, 204; wegen „ihrer politischen Dimension“ könnte die Beanstandung „durchaus ein wirksames Instrument sein, um über einen Einzelfall hinaus zur behördenübergreifenden, teilweise landesweiten Hebung des Datenschutzniveaus beizutragen“, *Petri*, Hdb. Sicherheits- und Staatschutzrecht, 667, 710 Rn. 101.

³⁴⁷ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 40.

³⁴⁸ *BfDI*, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 11; [32. Tätigkeitsbericht des BfDI](#) 2023, S. 92; „Sie scheitert allerdings dann, wenn die beanstandete Stelle und deren Fachaufsicht gleichgültig reagieren.“, *Petri*, Hdb. Sicherheits- und Staatsschutzrecht, 667, 710 Rn. 101.

³⁴⁹ *Stoklas/Wendorf*, ZD-Aktuell 2016, 5345.

³⁵⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 51, 52; kritisch waren bereits die Stellungnahmen der Datenschutzbeauftragten zu BVerfG, Urteil v. 14.7.1999 - 1 BvR 2420/95 - Rn. 141: „Alle Datenschutzbeauftragten halten ihre Kontrollmöglichkeiten für unzureichend.“

veranlasst.“ Dies sei insbesondere dann auffällig, wenn die Datenverarbeitung „auf eine[r] unzureichende[n] Rechtsgrundlage“ beruhe. In der Praxis würden rechtswidrige Zustände demnach trotz Beanstandung nicht abgestellt. Das sei der Grund, weshalb der BfDI seit langem „Abhilfebefugnisse“ fordere, „die sich an denjenigen der JI-Richtlinie orientieren, sodass als ultima ratio zum Beispiel auch eine Löschanordnung denkbar wäre.“ Zur endgültigen Klärung eines solchen Rechtsstreits könne über einen „besonderen Rechtsweg nachgedacht werden“.³⁵¹

Im Ergebnis ist die Beanstandung keine „wirksame Befugnis“, weil der rechtswidrige Zustand dadurch nicht immer beendet wird. Dass den Datenschutzbeauftragten keine abschließenden Entscheidungsrechte zustehen, ist daher verfassungswidrig.

d. Teilweise Unionsrechtswidrigkeit

Soweit für Teile der nachrichtendienstlichen Tätigkeiten nach der neuesten Rechtsprechung Unionsrecht anwendbar ist, müssen die Datenschutzbehörden gegenüber den Nachrichtendiensten zumindest Weisungen erteilen können.³⁵² Sie lediglich mit einem unverbindlichen Beanstandungsrecht auszustatten, ist insoweit unionsrechtswidrig.

7. Barrieren

Insbesondere zwei Barrieren sind für die Praxis der Datenschutzkontrolle hervorzuheben: die unzureichende Personalausstattung (a.) und die rechtlichen Kontrollhindernisse (b.).

a. Unzureichende personelle Ressourcen

Dass für die Datenschutzkontrolle der Nachrichtendienste zum Teil kein ausreichendes Personal vorhanden ist, wurde bereits erörtert.³⁵³ Daraus resultiert eine Barriere für wirksame Datenschutzkontrollen³⁵⁴, die spätestens dann verfassungswidrig ist, wenn keine regelmäßigen Kontrollen mehr erfolgen können³⁵⁵.

b. Rechtliche Kontrollhindernisse

Die Tätigkeit der Datenschutzbeauftragten begegnet verschiedenen rechtlichen Kontrollhindernissen.

³⁵¹ *Sosna*, GSZ 2022, 245, 247.

³⁵² Vgl. [Teil 2 B. II. 2. a. cc\)\(1\)](#).

³⁵³ Vgl. [Teil 3 D. II. 4. a.](#)

³⁵⁴ *Kutscha*, NVwZ 2003, 1296, 1299.

³⁵⁵ Vgl. [Teil 3 D. II. 3.](#)

aa) Ausnahmetatbestände

Die Kontrollmittel zur Informationsgewinnung gelten in vielen Ländern und auf der Bundesebene nicht uneingeschränkt.

So normiert § 28 Abs. 3 S. 3 BVerfSchG einen vollständigen Ausschluss der Kontrollrechte, da sie nicht durchsetzbar sind, „(...) soweit das Bundesministerium des Innern, für Bau und Heimat im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.“³⁵⁶ Die Norm gilt gem. § 62 BNDG und § 13a MADG auch für den BND und den MAD. Daher ist es beispielsweise jederzeit möglich, dass die Nachrichtendienste dem Kontrollbegehren des BfDI entgegenhalten, dass es sich um Daten eines ausländischen Nachrichtendienstes handle und eine Einsichtnahme deshalb wegen der Third Party Rule nicht erfolgen könne. Der BfDI berichtet, Daten aus dem Ausland zu überprüfen, sei „oftmals unmöglich“, weil der BND den Zugang zu diesen Daten mit Verweis auf die Third Party Rule verbiete.³⁵⁷ Offenbar beruft sich der BND auch auf die Third Party Rule, ohne eine Gefährdung für die Sicherheit gem. § 28 Abs. 3 S. 3 BVerfSchG geltend zu machen. Da ein solcher Ausnahmetatbestand gesetzlich nicht vorgesehen ist, ist diese Vorgehensweise rechtswidrig.

Weitere acht Landesgesetze enthalten ebenfalls einen vollständigen Ausschluss der Kontrollrechte.³⁵⁸ In Brandenburg kann der LfDI jedoch beantragen, dass die Verweigerung gegenüber dem „zuständigen Ausschuss“ des Landtags „in geheimer Sitzung“ begründet wird, anschließend wird der Ausschuss darüber entscheiden.³⁵⁹

In einigen Bundesländern gilt: Sofern eine oberste Landesbehörde bzw. das Innenministerium im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet, dürfen die Kontrollrechte ausschließlich von dem Datenschutzbeauftragten persönlich und teilweise zusätzlich von dessen Vertreter wahrgenommen werden.³⁶⁰

³⁵⁶ § 63 BNDG i. V. m. § 28 Abs. 3 S. 3 BVerfSchG und § 13 a MADG, § 28 Abs. 3 S. 3 BVerfSchG, wobei statt dem Innenministerium das Bundeskanzleramt oder das Bundesministerium der Verteidigung zuständig sind; Stellungnahme des BfDI *Kelber* i.R.v. BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 293, der schreibt, Daten aus dem Ausland zu überprüfen, sei „oftmals unmöglich“, weil der Bundesnachrichtendienst den Zugang zu diesen Daten mit Verweis auf die Third Party Rule verbiete.

³⁵⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 293.

³⁵⁸ § 17 Abs. 2 S. 2 [BWLVS](#); § 30 Abs. 2 [LVerfSchG RP](#), offenbar darf in der Praxis dann jedoch zumindest der LfDI Einsicht nehmen; § 15 Abs. 3 S. 3 [VSG NRW](#); § 23b Abs. 3 S. 3 [HmbVerfSchG](#); § 36 [ThürVerfSchG](#), § 7 Abs. 5 S. 2 [ThürDSG](#); § 32a Abs. 3 S. 3 [VSG Bln](#); § 30 [VerfSchG-LSA](#), § 23 Abs. 2 S. 2 [DSG-LSA](#) in der Fassung der Bekanntmachung vom 13. Januar 2016; § 27 Abs. 1 Nr. 1 [BbgVerfSchG](#), § 21 Abs. 2 [BbgDSG](#); Art. 32 Abs. 2 [BayVSG](#), Art. 16 Abs. 2 S. 2 [BayDSG](#).

³⁵⁹ § 27 Abs. 1 Nr. 1 [BbgVerfSchG](#), § 21 Abs. 2 S. 2 [BbgDSG](#).

³⁶⁰ § 15 Abs. 1 Nr. 1 [HVSG](#), § 14 Abs. 5 S. 1 [HDSIG](#), die in § 15 Abs. 5 S. 2 normierte Ausnahme auch gegenüber dem LfDI dürfte im Nachrichtendienstrecht i.d.R. keine Rolle spielen, weil die betroffenen

Nur in den zwei Bundesländern, Bremen und Sachsen, können die Kontrollmittel nicht ausgeschlossen werden, sie stehen den Datenschutzbeauftragten daher uneingeschränkt zu.

(1) Unwirksamkeit der Befugnisse

Nach der Rechtsprechung des Bundesverfassungsgerichts müssen die Datenschutzbeauftragten über „wirksame Befugnisse“ verfügen.³⁶¹ Über Ausnahmen von diesen Befugnissen spricht das Bundesverfassungsgericht nicht. Andererseits impliziert der Begriff der Wirksamkeit auch keinen maximalen Befugnisbestand. Stattdessen stellt er eine qualitative Bedingung an die Ausgestaltung der durch den Gesetzgeber verliehenen Befugnisse: sie müssen wirksam sein. Das sind sie nur, wenn der beabsichtigte Erfolg tatsächlich eintritt.³⁶²

In der Literatur wird betont, dass die Ausnahmeklausel nur in seltenen Ausnahmefällen angewandt werden sollte, weil die Datenschutzbeauftragten erstens wegen ihrer Wahl durch das Parlament besonders legitimiert sind und zweitens eine Gefährdung erst bei einer Veröffentlichung der Informationen gegenüber der Öffentlichkeit, nicht jedoch bereits durch die Kenntnisnahme des Datenschutzbeauftragten entstehe.³⁶³ Ob der Sicherheitsvorbehalt – entsprechend der Forderungen aus der Wissenschaft – tatsächlich sehr eng ausgelegt wird, ist wegen der absoluten Geheimhaltung der Vorgänge nicht nachvollzieh- und kontrollierbar.

Da die Sicherheit des Bundes oder eines Landes im Nachrichtendienstrecht aufgrund der Natur des Auftrags durch eine Erweiterung der Kenntnisträger häufig bedroht sein wird und dieser Ausnahmetatbestand deshalb potenziell jederzeit erfüllt ist, ist der in neun Gesetzen vorgesehene vollständige Ausschluss der Kontrollrechte verfassungswidrig. Die Ausnahme-Generalklausel ist sprachlich so weit gefasst, dass sie keinerlei begrenzende Wirkung mehr entfaltet. Der beabsichtigte Erfolg der Kontrollmittel kann dann nicht mehr eintreten, was sie zu unwirksamen Befugnissen werden lässt. Die weitreichende Ausnahme verkennt zudem die verfassungsrechtliche Herleitung und Notwendigkeit des Kontrollmechanismus: Die Datenschutzkontrolle heimlicher

Personen von der Datenverarbeitung keine Kenntnis haben und daher keine Vertraulichkeitsvereinbarung schließen können, denkbar ist dessen Geltendmachung nur in Bezug auf Vertrauenspersonen; § 33a Abs. 2 S. 3 [NVerfSchG](#); § 3 Abs. 1, § 20 Abs. 4 S. 3 [SDSG](#), bei § 20 Abs. 4 S. 4 [SDSG](#) gilt das zu § 15 Abs. 5 S. 2 [HDSIG](#) Gesagte entsprechend; § 2 Abs. 7 Nr. 1, § 18 Abs. 2 [LD SG SH](#), wonach der Datenschutzbeauftragte und die „schriftlich besonders damit betrauten Beauftragten“ die Rechte wahrnehmen können. Hier stellt sich die Frage, ob darin überhaupt eine Einschränkung liegt.

³⁶¹ Vgl. [Teil 2 A. III. 1. a. gg.](#)

³⁶² Vgl. [Teil 2 A. III. 1. a. gg.](#)

³⁶³ [Kornblum](#), Rechtsschutz, S. 81 f. m. w. N.

nachrichtendienstlicher Datenverarbeitung grundsätzlich vorzusehen, ist kein großzügiges Entgegenkommen des Gesetzgebers, sondern eine zwingende Voraussetzung für die Verhältnismäßigkeit der Maßnahmen.

Gusy hat daher zu Recht bereits 1990 betont, dass es „schlechterdings nicht nachvollziehbar“ ist, inwiefern die Einsichtnahme durch den BfDI die Sicherheit des Staates beeinträchtigen könne. Da der BfDI zur Amtsverschwiegenheit verpflichtet ist, bestehe keine Gefahr, dass er sicherheitsempfindliche Informationen im öffentlichen Datenschutzbericht veröffentliche. Mit dem Ausnahmetatbestand würden „kontrollfreie Räume geschaffen“. Dies sei mit Art. 19 Abs. 4 GG nicht vereinbar.³⁶⁴

Darüber hinaus stehen die weitreichenden Ausnahmetatbestände auch in einem systematischen Widerspruch zu den Normen zur G 10-Kommission, die ebenfalls ein Datenschutzkontrollleur ist: Für deren Kontrollrechte gelten gerade keine Grenzen. Dabei ist hervorzuheben, dass für die Datenschutzbeauftragten dieselben Verschwiegenheitsverpflichtungen gelten wie für die G 10-Kommission.

(2) Lösungsmöglichkeiten

Um die aufgezeigten verfassungswidrigen Regelungen zu entschärfen oder aufzulösen, gäbe es mehrere Optionen.

Wenn die Kontrollrechte (in verfassungswidriger Weise) nicht vorbehaltlos gewährleistet werden sollen³⁶⁵, sollten zumindest die Einzelfälle, in denen eine Kontrolle verwehrt werden kann, bereits im Gesetz konkretisiert und detaillierter beschrieben werden. So könnte man klarstellen, dass gegebenenfalls die Third Party Rule einer Kontrolle entgegenstehen kann³⁶⁶. Dass die Kontrollrechte nicht gehäuft verweigert und damit unwirksam werden, müsste dann durch eine Ausgestaltung nach dem brandenburgischen Modell abgesichert werden, wo der LfDI das PKGr um Entscheidung über die Auskunft bitten kann.³⁶⁷ Gegen diese Lösungsmöglichkeit spricht, dass die Kontrolle gegenüber unabhängigen Institutionen der Rechtskontrolle nicht verwehrt werden darf. Daher wäre es empfehlenswerter, die Kontrollrechte entsprechend dem Regelungsmodell in einigen Bundesländern in besonderen Ausnahmefällen nicht auszuschließen, sondern auf den Datenschutzbeauftragten persönlich zu beschränken und

³⁶⁴ *Gusy*, Richterliche Kontrolle, 67, 90.

³⁶⁵ Anzumerken ist, dass die Geheimhaltungsbedürfnisse insoweit wesentlich überzeugender vorgebracht werden könnten, wenn nicht die Nachrichtendienste selbst in großem Umfang private Unternehmen in ihre Arbeitsweisen einweihen und einbeziehen würden, die im Gegensatz zu den Kontrolleuren keine grundlegende Bedeutung für die Entfaltung des Rechtsstaatsprinzips haben, <https://www.sueddeutsche.de/politik/bnd-afghanistan-reform-1.5449520> vom 26.10.2021 (abgerufen am 31.8.2024).

³⁶⁶ Näher zur Third Party Rule, vgl. [Teil 2 A. III. 1. a. II](#)), [Teil 2 A. III. 1. b. II](#)), [Teil 3 B. XII. 2.](#)

³⁶⁷ Vgl. [Teil 3 D. II. 7. b. aa](#).

eine Kenntnisnahme durch die von ihm Beauftragten auszuschließen.³⁶⁸ So bleibt der Kreis der Geheimnisträger sehr klein, ohne dass von der verfassungsrechtlich erforderlichen externen Kontrolle abgesehen wird.

Die Ausnahmen sollten jedoch vollständig gestrichen werden, weil die Aufsichtsbehörden über die Einschlägigkeit der Ausnahme selbst entscheiden, obwohl sie es sind, die die politische Verantwortung für die Maßnahme tragen. Dadurch können sie selbst die „Möglichkeiten und Grenzen ihrer Überwachung“ bestimmen³⁶⁹, was dem Zweck der Kontrolle zuwiderläuft. Mithin ist diese Möglichkeit des Kontrollierten geeignet, „die Wirksamkeit des gesamten Kontrollsystems in Frage zu stellen“.³⁷⁰

bb) Zuständigkeitsvorbehalt zugunsten der G 10-Kommission

Für die Kontrolle bestimmter Datenverarbeitungen der Nachrichtendienste sind die Datenschutzbeauftragten rechtlich nicht zuständig.

Neun Nachrichtendienstgesetze legen fest, dass die Kontrollkompetenz der Datenschutzbeauftragten beschränkt ist, soweit die Verarbeitung von Daten der Kontrolle durch die G 10-Kommission unterliegt.³⁷¹ Soweit der Anwendungsbereich von Art. 10 GG eröffnet ist oder den G 10-Kommissionen weitere Aufgaben übertragen wurden³⁷², können die Datenschutzbeauftragten bestimmte Vorgänge daher nicht kontrollieren.

Auf der Bundesebene wird § 28 Abs. 2 BVerfSchG (§ 26 a BVerfSchG a.F.) so interpretiert, dass Doppelzuständigkeiten zwar vermieden werden sollen, eine Kenntnisnahme des BfDI bei Daten, für deren Kontrolle die G 10-Kommission zuständig ist, jedoch nicht ausgeschlossen werden soll, soweit dies im Rahmen einer Prüfung erforderlich ist.³⁷³ Diese Kenntnis ist für die Tätigkeit des Datenschutzbeauftragten zwingend, weil der BfDI für die Kontrolle von Vorgaben zuständig bleibt, die außerhalb des Auftrags der G 10-Kommission liegen.³⁷⁴ Insoweit muss beachtet werden, dass die

³⁶⁸ So auch *Aden*, Vorgänge 2015, 245, 248.

³⁶⁹ *Gusy*, Richterliche Kontrolle, 67, 90; *Kauß*, Der suspendierte Datenschutz, S. 282.

³⁷⁰ *Kauß*, Der suspendierte Datenschutz, S. 282.

³⁷¹ § 28 Abs. 2 S. 2 BVerfSchG (§ 63 BNDG bzw. § 13 a MADG, § 28 Abs. 2 S. 2 BVerfSchG); § 6 Abs. 1 [AG G 10 RP](#); § 30 Abs. 1 S. 2 [LVerfSchG RP](#); § 17 Abs. 1 S. 2 [BWLVS](#); § 15 Abs. 2 S. 3 [VSG NRW](#); § 23b Abs. 2 S. 2 [HmbVerfSchG](#); § 39 Abs. 1 S. 1 [SächsVSG](#); Umkehrschluss aus § 5 Abs. 3 S. 1 [AG G 10-LSA](#); § 3 Abs. 1 [AG G 10 MV](#); § 32a Abs. 2 S. 2 [VSG Bln](#); *Aden*, Vorgänge 2015, 245, 248.

³⁷² Vgl. [Teil 3 B. II. 3.](#)

³⁷³ BT-Drs. 18/11325, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 v. 24.2.2017, S. 122, 123; *Sosna*, GSZ 2022, 245, 249; vgl. zur alten Rechtslage noch der [24. Tätigkeitsbericht des BfDI](#) v. 24.4.2013, S. 105.

³⁷⁴ *Warg*, Recht der Nachrichtendienste, S. 98 Rn. 224; Schenke/Graulich/Ruthig/*Siems*, § 26a BVerfSchG Rn. 7.

G 10-Kommission ausschließlich die Einhaltung des G 10 prüft und nur im Ausnahmefall, bei der Kontrolle von Auskunftsverlangen und dem Einsatz von IMSI/IMEI-Catchern, auch Vorgaben des BVerfSchG.³⁷⁵

Damit ist der BfDI für die Kontrolle nicht zuständig, soweit die G 10-Kommissionen die Vereinbarkeit mit dem G 10 (oder dem BVerfSchG) prüft³⁷⁶, kann sich jedoch über den Ist-Zustand informieren, um seinen Kontrollaufgaben gerecht werden zu können.

III. Parallele Zuständigkeit bei der strategischen Ausland-Fernmeldeüberwachung und bei Eingriffen in informationstechnische Systeme von Ausländern im Ausland

Für die Kontrolle von Datenverarbeitungen im Rahmen der strategischen Ausland-Fernmeldeaufklärung und von Eingriffen in informationstechnische Systeme von Ausländern im Ausland sind sowohl das AdKon des UKRats³⁷⁷ als auch der BfDI zuständig.³⁷⁸ Während § 63 BNDG i. V. m. § 28 Abs. 2 BVerfSchG eine Zuständigkeit des BfDI ausschließt, soweit die G 10-Kommission zuständig ist, wurde eine solche Regelung zugunsten des UKRats nicht geschaffen. Schon während des Gesetzgebungsverfahrens hatten Experten kritisch auf die insoweit parallele Zuständigkeit des AdKon und des BfDI hingewiesen.³⁷⁹ Trotzdem hat man die Doppelzuständigkeit beibehalten: § 58 Abs. 4 BNDG stellt klar, dass die Rechte des BfDI „von der Tätigkeit des Unabhängigen Kontrollrats unberührt“ bleiben.

Eine Kooperation zwischen den beiden Kontrolleuren ist nur im Ansatz vorgesehen. So können sich der UKRat, die G 10-Kommission und der BfDI lediglich über allgemeine Angelegenheiten austauschen (§ 58 Abs. 3 BNDG). Die Begrenzung auf „allgemeine Angelegenheiten“ verhindert eine inhaltliche Zusammenarbeit, mit deren Hilfe Kontrolllücken und doppelte Kontrollen vermeidbar wären.³⁸⁰ Anders als die G 10-Kommission kann der UKRat den BfDI auch nicht beauftragen, „die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten“ (§ 28 Abs. 3 S. 2 BVerfSchG).

³⁷⁵ Vgl. [Teil 3 B. II. 1. a.](#)

³⁷⁶ *Bäcker*, Beschwerdeschrift G 10, S. 68.

³⁷⁷ Vgl. [Teil 3 C. II. 2. a.](#)

³⁷⁸ *Löffelmann/Zöller*, Nachrichtendienstrecht, S. 263; *Sosna*, GSZ 2022, 245, 250.

³⁷⁹ Im Detail vgl. [Teil 4 B. I. 1. b.](#); *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 25; *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15.

³⁸⁰ *BfDI*, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 10; darüber hinaus schlägt *Wetzling* weitere Zusammenarbeitsmöglichkeiten vor, *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15.

Im Ergebnis kontrollieren das AdKon und der BfDI Datenverarbeitungen im Zusammenhang mit der strategischen Ausland-Fernmeldeaufklärung jeder für sich, und zwar nebeneinanderher. Daher ist es wahrscheinlich, dass der BND bestimmte Praktiken oder Vorgänge jeweils beiden Kontrolleuren vorlegen und erörtern muss. Selbst wenn die beiden Kontrolleure Mehrfachbelastungen des BND verhindern wollen würden, würde dies das Gesetz nicht zulassen, weil sie sich über einzelne Vorgänge nicht austauschen dürfen.

E. Die Kernbereichsschutzkonzepte

Es gibt bundesweit kein Kernbereichsschutzkonzept, das die verfassungsrechtlichen Anforderungen³⁸¹ erfüllt. Die Verfassungsschutzgesetze von Berlin und Mecklenburg-Vorpommern enthalten kein Kernbereichsschutzkonzept, sie sind daher offensichtlich verfassungswidrig. Teilweise gibt es allgemeine Kernbereichsschutznormen³⁸², teilweise werden die Kernbereichsschutzvorgaben in bestimmte nachrichtendienstliche Befugnisse integriert³⁸³, vereinzelt werden beide Regelungsmodelle miteinander kombiniert³⁸⁴.

Im Folgenden wird beantwortet, inwieweit die verfassungsrechtlich zwingende Einbindung einer unabhängigen Stelle auf der Auswertungsebene verwirklicht ist.

I. Ausgestaltung der (unabhängigen) Stelle

Wie die unabhängige Stelle gesetzlich ausgestaltet wurde, variiert deutlich.

1. Keine Stelle

In den Kernbereichsschutznormen der Verfassungsschutzgesetze von Sachsen-Anhalt und Schleswig-Holstein ist auf der Auswertungsebene keine Stelle vorgesehen, was diese Regelungen verfassungswidrig macht. Dass dem LfV Schleswig-Holstein keine Befugnis zur Wohnraumüberwachung oder Online-Durchsuchung verliehen wurde,

³⁸¹ Vgl. [Teil 2 A. III. 2.](#)

³⁸² § 3a G10, §§ 22, 36 BNDG; § 5a VSG NRW; § 7a BbgVerfSchG; § 8a BremVerfSchG; § 10 NVerfSchG; spezieller Absatz innerhalb einer allgemeinen Norm zu nachrichtendienstlichen Mitteln § 7 Abs. 1a HmbgVerfSchG; § 10 ThürVerfSchG; § 8 Abs. 3a, b VerfSchG-LSA; § 8 Abs. 4 LVerfSchG SH.

³⁸³ § 5d Abs. 3 BWLVSG; § 18 Abs. 6 LVerfSchG RP; § 8 SächsVerfSchG; § 8 Abs. 3 SVerfSchG.

³⁸⁴ § 14, § 7 Abs. 5, § 11 Abs. 7, § 12 Abs. 4, 5, 7, § 13 Abs. 1 HVSG; Art. 8a BayVSG.

ändert daran nichts, weil auch beim Einsatz von Verdeckten Ermittlern oder Vertrauensleuten in Zweifelsfällen eine Sichtung durch den behördlichen Datenschutzbeauftragten erfolgen muss³⁸⁵, die hier nicht vorgeschrieben ist.

2. Keine unabhängige Stelle

In manchen Fachgesetzen ist zwar eine Sichtung vorgesehen, die beauftragte Stelle ist jedoch besetzt mit einem Mitarbeiter des Nachrichtendienstes, der lediglich nicht identisch mit dem Beschaffer bzw. Auswerter ist. Häufig wird ein „unabhängiger, besonders bestellter Bediensteter“ mit „Befähigung zum Richteramt“ eingebunden.³⁸⁶ In Thüringen entscheidet in Zweifelsfällen zusätzlich die Stabsstelle Controlling, eine beim Präsidenten des Landesamts für Verfassungsschutz angesiedelte Abteilung, die unter anderem die Zweck- und Rechtmäßigkeit von Maßnahmen überprüft und nicht weisungsgebunden ist (§ 2 ThürVerfSchG).³⁸⁷ Teilweise sind der Leiter des Verfassungsschutzes³⁸⁸ oder der behördliche Datenschutzbeauftragte³⁸⁹ als Stelle benannt.

Dass die verfassungsrechtlichen Anforderungen an die Unabhängigkeit der Kontrolleure dadurch nicht erfüllt werden, ergibt sich aus der Rechtsprechung, denn das Bundesverfassungsgericht hat festgelegt, dass die Stelle „unabhängig“ und „nicht mit Sicherheitsaufgaben betraut“ sein darf. Die als unabhängige Stellen vorgesehenen Mitarbeiter der Nachrichtendienste sind jedoch zweifellos mit Sicherheitsaufgaben „betraut“. Zudem stehen diese Ausgestaltungen im Widerspruch zum Zweck der Vorgabe, der gerade darin besteht, dass diese Daten *vor* der Kenntnisnahme durch die Behörde herausgefiltert werden.³⁹⁰ Wenn die Stelle mit Mitarbeitern der Behörde besetzt ist, erlangt die Behörde durch ihre Mitarbeiter automatisch Kenntnis, so dass bei dieser extensiven Auslegung der Unabhängigkeit der Zweck nicht mehr erfüllt werden kann. Bei der Auswertung von Daten aus einem Eingriff in informationstechnische Systeme lässt das Bundesverfassungsgericht explizit zu, dass Bedienstete des Nachrichtendienstes bei

³⁸⁵ Vgl. [Teil 2 A. III. 2.](#)

³⁸⁶ § 10 Abs. 2 S. 2 [NVerfSchG](#); gem. § 5a Abs. 3 [VSG NRW](#), § 8a Abs. 2 S. 2 [BremVerfSchG](#) zwar nicht eigenverantwortlich, sondern nur zusätzlich zur unabhängigen G 10-Kommission, das ändert jedoch nichts an der Kenntnisnahme durch diesen Mitarbeiter, die es eigentlich zu verhindern gilt.

³⁸⁷ § 10 Abs. 6 S. 8 [ThürVerfSchG](#).

³⁸⁸ § 10 Abs. 5 [NVerfSchG](#); § 7 Abs. 1a S. 5 [HmbgVerfSchG](#), wobei die Verarbeitung nur fortgesetzt werden darf, wenn das PKGr „unterrichtet“ wurde; Gem. § 7a Abs. 5 [BbgVerfSchG](#) zwar nicht eigenverantwortlich, sondern nur zusätzlich zur unabhängigen G 10-Kommission, das ändert jedoch nichts an der Kenntnisnahme durch diese Person, die es eigentlich zu verhindern gilt.

³⁸⁹ § 14 Abs. 5 S. 3, § 12 Abs. 4, 5, 7, § 13 Abs. 1 [HVSG](#), wobei gem. § 7 Abs. 5 u.a. für die Wohnraumüberwachung eine gerichtliche Prüfung vorgeschrieben ist, sodass die Einbindung des behördlichen Datenschutzbeauftragten keinen Verfassungsverstoß darstellt, weil bei den einschlägigen nachrichtendienstlichen Mitteln eine Kontrolle durch eine unabhängige Stelle jedenfalls nicht zwingend notwendig ist.

³⁹⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 278.

der Sichtung eingebunden werden, wenn die unabhängige Stelle an technische und fachliche Grenzen stößt, solange die tatsächliche Durchführung und die Entscheidungsverantwortung „maßgeblich in der Verfassungsschutzbehörde gegenüber unabhängigen Händen liegen“³⁹¹. Diese Erläuterung wäre sinnlos, wenn Bedienstete des Nachrichtendienstes generell eingebunden werden könnten. Unabhängig im Sinne der Rechtsprechung kann daher nur eine externe Stelle sein.

Weil diese Normen eine Kenntnisnahme kernbereichsrelevanter Daten durch Mitarbeiter des Nachrichtendienstes ermöglichen, sind sie eindeutig verfassungswidrig.

3. Unabhängige Stellen

Es gibt im Bundesvergleich insgesamt drei unterschiedliche unabhängige Stellen, die (potenziell) kernbereichsrelevante Daten sichten: Für die Sichtung von Kernbereichsdaten aus der strategischen Ausland-Fernmeldeaufklärung und Eingriffen in informationstechnische Systeme von Ausländern im Ausland durch den BND ist der UKRat zuständig³⁹², darüber hinaus ist auf der Bundesebene und in fünf Bundesländern die G 10-Kommission³⁹³ die unabhängige Stelle, in vier weiteren Bundesländern ist ein Gericht mit der Sichtung betraut³⁹⁴.

II. Reichweite der Einbindung

Die Fachgesetze, nach deren Kernbereichsschutzvorkehrungen eine unabhängige Stelle eingebunden wird, tun dies in sehr unterschiedlichem Umfang.

Am weitestgehenden ist die Einbindung der unabhängigen Stellen in Bayern und in Brandenburg, denn sie entscheiden immer über die Verwertbarkeit von erhobenen kernbereichsrelevanten Daten, unabhängig davon, mit welcher nachrichtendienstlichen Befugnis die Daten erlangt wurden. Die sächsische Regelungsweise ist zwar ähnlich, hier entscheidet jedoch beim Einsatz von Verdeckten Ermittlern und Vertrauensleuten nur der behördliche Datenschutzbeauftragte über die Verwertbarkeit, bei allen anderen nachrichtendienstlichen Befugnissen ist die unabhängige Stelle zuständig.³⁹⁵

³⁹¹ Vgl. [Teil 2 A. III. 2. b.](#)

³⁹² §§ 22, 36 Abs. 3 BNDG.

³⁹³ § 3a Abs. 1 S. 4, 5 G 10; § 5d Abs. 3 S. 1 [BWLVS](#); § 3a Abs. 1 S. 4, 5 G 10; § 18 Abs. 6 S. 3 [LVersSchG RP](#); § 5a Abs. 5 [VSG NRW](#); § 7a Abs. 2 S. 5 [BbgVerfSchG](#); § 3a Abs. 1 S. 4, 5 G 10; § 8a Abs. 5 S. 1 [BremVerfSchG](#).

³⁹⁴ § 8 Abs. 3 S. 4 [SVerfSchG](#); Art. 8a S. 3, Art. 11 Abs. 2 S. 3 [BayVSG](#); § 7 Abs. 5, § 11 Abs. 7 [HVSG](#); § 8 Abs. 3 S. 4 [SächsVerfSchG](#), hier ist bei Entscheidungen über Zweifelsfälle jedoch der behördliche Datenschutzbeauftragte zuständig, vgl. z.B. § 11 Abs. 6 S. 4

³⁹⁵ Art. 8a Abs. 1 S. 5, § 11 Abs. 2 S. 3 [BayVSG](#); § 7a Abs. 2 S. 5 [BbgVerfSchG](#); § 8 Abs. 3 S. 5, §§ 11 Abs. 6 S. 5, § 12 Abs. 1 [SächsVerfSchG](#).

In zwei Bundesländern ist die unabhängige Stelle ausschließlich bei durch die Wohnraumüberwachung erhobenen Daten eingebunden.³⁹⁶ Nach dem Hessischen Verfassungsschutzgesetz wird das Gericht tätig, wenn im Rahmen einer Wohnraumüberwachung oder längerfristigen Observation potenziell kernbereichsrelevante Informationen verwendet werden sollen.³⁹⁷

Nach diesen Konzepten erfasst die Kontrolle entsprechend den Rechtsprechungsvorgaben die Wohnraumüberwachung bzw. in Bayern, wo eine Online-Durchsuchung möglich ist, auch die Online-Durchsuchung.³⁹⁸ In Nordrhein-Westfalen, wo der Verfassungsschutz zur Wohnraumüberwachung nicht ermächtigt ist, wird die unabhängige Stelle bei in Art. 10 GG eingreifenden Maßnahmen eingebunden (§ 5a Abs. 5 VSG NRW).

Demgegenüber ist die Rechtslage auf der Bundesebene, in Baden-Württemberg und Bremen verfassungswidrig, weil eine unabhängige Sichtung bei kernbereichsrelevanten Daten aus der Wohnraumüberwachung nicht vorgesehen ist.

III. Art der Einbindung

1. Wohnraumüberwachung und Online-Durchsuchung

Die sechs Regelungen, die eine Sichtung durch eine unabhängige Stelle vorsehen, unterscheiden sich in der Frage, wann und mit welchem Auftrag die unabhängige Stelle tätig wird. Für Daten aus der Wohnraumüberwachung und aus Online-Durchsuchungen hat das Bundesverfassungsgericht entschieden, dass sämtliche durch diese Maßnahmen gewonnenen Daten vollständig gesichtet werden müssen³⁹⁹.

Die zwei im Jahr 2023 novellierten Verfassungsschutzgesetze in Bayern und Hessen erfüllen diese Voraussetzungen, denn dort ist festgelegt, dass die unabhängige Stelle bzw. das Gericht über die Verwertbarkeit aller erhobenen Daten bzw. Aufzeichnungen entscheidet.⁴⁰⁰ Nach dem sächsischen Verfassungsschutzgesetz gilt dies zumindest für die Wohnraumüberwachung (§ 10 Abs. 2 SächsVSG).

³⁹⁶ § 18 Abs. 6 S. 3 [LVerfSchG RP](#); § 8 Abs. 3 S. 4 [SVerfSchG](#).

³⁹⁷ § 7 Abs. 5, § 11 Abs. 7 [HVSG](#).

³⁹⁸ Zu Online-Durchsuchungen sind diese Verfassungsschutzbehörden ohnehin nicht berechtigt.

³⁹⁹ Vgl. [Teil 2 A. III. 2. b. aa](#).

⁴⁰⁰ § 11 Abs. 7 [HVSG](#), vgl. auch Hessischer Landtag Drs. 20/10821 v. 21.3.2023, S. 27; Art. 11 Abs. 2 S. 3 [BayVSG](#), vgl. auch den Gesetzesentwurf der Landesregierung v. 13.12.2022, S. 35, https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwuerfe/%C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 15.2.2024).

In Bayern kann das Gericht im Rahmen dieser Kontrolle auf der Auswertungsebene Mitarbeiter des bayerischen Landesamts zu Rate ziehen. Dafür wird beim LfV eine „unterstützende Datenprüfstelle“ eingerichtet, deren Mitarbeiter „im Rahmen der Weisungen des Gerichts unabhängig“ und „in eigener Verantwortung“ tätig sind (Art. 31 BayVSG). Diese Neuregelung beruht auf einer Formulierung des Bundesverfassungsgerichts, wonach eine Hinzuziehung von Bediensteten des LfV zur „Gewährleistung von ermittlungsspezifischem Sachverstand“ und zur „technische[n] Unterstützung“ nicht ausgeschlossen sei, solange die „tatsächliche Durchführung und die Entscheidungsverantwortung (...) maßgeblich in (...) unabhängigen Händen“ läge.⁴⁰¹

Nach den anderen drei Regelungen, also in Brandenburg, Rheinland-Pfalz, Sachsen und dem Saarland, müssen die Daten nur dann der unabhängigen Stelle vorgelegt werden, wenn Zweifel bestehen, ob die erhobenen Daten kernbereichsrelevant sind.⁴⁰² Das Bundesverfassungsgericht hatte Art. 8a Abs. 1 der alten Fassung des Bayerischen Verfassungsschutzgesetzes, die § 3a Abs. 1 S. 4 G 10 für anwendbar erklärte, mit folgender Begründung als verfassungswidrig beurteilt:

„Mit diesem Verweis ist jedoch nicht sichergestellt, dass die Daten aus einer Wohnraumüberwachung vollständig vorgelegt werden. Der entsprechend anzuwendende § 3a Abs. 1 Satz 4 G 10 betrifft nach seinem Wortlaut nur automatische Aufzeichnungen nach § 3a Abs. 1 Satz 3 G 10. Das sind Aufzeichnungen, die angefertigt werden, wenn im Rahmen einer (Telekommunikations-)Überwachung zunächst eine unmittelbare Kenntnisaufnahme erfolgt, diese aber unterbrochen werden muss und nur eine automatische Aufzeichnung fortgesetzt werden darf, weil Zweifel bestehen, ob nicht Inhalte erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind (vgl. § 3a Abs. 1 Satz 2 und Satz 3 G 10). Den Anforderungen des Art. 13 GG an den Kernbereichsschutz bei einer akustischen oder optischen Wohnraumüberwachung ist indessen nur genügt, wenn sämtliche Daten, die aus der Überwachung erlangt wurden, zunächst zur unabhängigen Sichtung vorgelegt werden. Dazu zählen auch Daten, die erhoben wurden, ohne dass die Behörde Zweifel hatte, dass keine kernbereichsrelevanten Daten enthalten seien, in denen sie mit anderen Worten annahm, nicht durch den Kernbereichsschutz an der Erhebung gehindert zu sein.“⁴⁰³

⁴⁰¹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 316.

⁴⁰² § 7a Abs. 2 S. 5 [BbgVerfSchG](#), § 3a S. 4, 5 G10; § 18 Abs. 6 S. 3 [LVerfSchG RP](#), § 3a S. 4, 5 G10; § 5a Abs. 4 S. 2 [SächsVerfSchG](#); § 8 Abs. 3 S. 4 [SVerfSchG](#).

⁴⁰³ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 306.

Die drei genannten Regelungen, die eine Vorlage nur für Zweifelsfälle vorsehen, sind nach der zitierten Rechtsprechung des Bundesverfassungsgerichts verfassungswidrig.

2. Strategische Ausland-Fernmeldeüberwachung und Eingriffe in informationstechnische Systeme von Ausländern im Ausland

Bei Daten aus der strategischen Ausland-Fernmeldeaufklärung hat das Bundesverfassungsgericht abweichend von den zitierten Vorgaben einen niedrigeren Schutz vorausgesetzt: insoweit ist es ausreichend, wenn auf der Auswertungsebene „die weitere Auswertung unverzüglich unterbrochen“ wird, sobald erkennbar ist, „dass eine Überwachung in den Kernbereich persönlicher Lebensgestaltung eindringt; schon bei Zweifeln darf ihre Fortsetzung – vorbehaltlich von Regelungen für Eilfälle (...) nur in Form von Aufzeichnungen erlaubt werden, die vor ihrer Auswertung von einer unabhängigen Stelle zu sichten sind.“⁴⁰⁴ Da eine solche Kontrolle durch das GeKon für die strategische Ausland-Aufklärung vorgesehen ist, sind diese Regelungen verfassungskonform.

Für Online-Durchsuchungen hat das Bundesverfassungsgericht wegen ihrer sehr hohen Eingriffsintensität jedoch vorgeschrieben, dass alle erhobenen Daten zunächst durch eine unabhängige Stelle zu sichten sind.⁴⁰⁵ Es ist unklar, ob diese Maßgabe auf Eingriffe in informationstechnische Systeme von Ausländern im Ausland durch den BND übertragbar ist. Dafür spricht, dass die Rechtsgrundlage Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen ermöglicht⁴⁰⁶. Misst man die Regelung in § 36 Abs. 3 BNDG an den Vorgaben zur Online-Durchsuchung, ist sie verfassungswidrig, weil die Norm – wie bei Daten aus der strategischen Ausland-Fernmeldeaufklärung – erst auf der Auswertungsebene und nur bei Zweifelsfällen eine Kontrolle vorschreibt. Das Bundesverfassungsgericht hat zwar entschieden, dass das grundrechtliche Schutzniveau von Ausländern im Ausland abgesenkt sein kann.⁴⁰⁷ Mit Blick auf die Absolutheit der Menschenwürde, die zu schützen die Wahrung eines Kernbereichs privater Lebensgestaltung bestimmt ist⁴⁰⁸, kann dies allerdings nicht für die Kernbereichsschutzvorkehrungen gelten. Weil die geltende Rechtsgrundlage für Eingriffe in informationstechnische Systeme von Ausländern im Ausland auch Online-Durchsuchung ermöglicht, müssen alle erhobenen Daten gesichtet werden. Die aktuelle Regulationsweise ist verfassungswidrig.

⁴⁰⁴ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 200.

⁴⁰⁵ Vgl. [Teil 2 A. III. 2. b. aa\).](#)

⁴⁰⁶ Vgl. [Teil 2 A. III. 4. b. aa\) \(2\).](#)

⁴⁰⁷ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 104.

⁴⁰⁸ Vgl. [Teil 2 A. II.](#), [Teil 2 A. III. 2.](#)

Sollte der Gesetzgeber die Norm zukünftig differenzierter regeln, könnte er die aktuelle Regelung für die Maßnahmen, die nur begrenzt mit der Online-Durchsuchung im klassischen Sinn vergleichbar sind⁴⁰⁹, übernehmen.

F. Kontroll-Gesamtüberblick

Nach Ansicht des Bundesverfassungsgerichts muss eine Kontrollinstitution „jedenfalls alle Überwachungsmaßnahmen, denen eine Person durch eine Behörde ausgesetzt ist, in den Blick nehmen“ können. Diese Vorgabe sei zwingend, weil der Kontrolleur die Verhältnismäßigkeit einer Maßnahme der Nachrichtendienste vor dem Hintergrund des Konzepts der additiven Eingriffswirkung nur bewerten könne, wenn er weiß, welchen zusätzlichen Maßnahmen der Betroffene ausgesetzt ist.⁴¹⁰

Die Bund-Länder-Arbeitsgruppe der Innenminister-Konferenz⁴¹¹, die das Urteil zum bayerischen Verfassungsschutzgesetz analysiert und Regelungsmodelle entwickelt hat, vertritt eine andere Auffassung als das Bundesverfassungsgericht. Dass eine unabhängige Kontrolle „fallbezogen Kenntnis über sämtliche Intensiveingriffe“ besitzt, sei aus der grundrechtlichen Schutzperspektive „nicht vorzugswürdig“, weil die „(unangefochtenen) aktuellen Regelungen schon verfassungsimmanent unterschiedliche Zuständigkeiten ermöglichen“, indem beispielsweise für „TKÜ-Maßnahmen die G 10-Kommission zuständig und für die Wohnraumüberwachung die richterliche Anordnung vorgeschrieben sei“.⁴¹²

Dass die Verfassung in Art. 10 Abs. 2 S. 2 GG die „Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane“ und in Art. 13 Abs. 3, 4 GG einen Richtervorbehalt vorsieht, und damit „unterschiedliche Zuständigkeiten“ ermöglicht, kann nicht als Argument dagegen dienen, dass eine Stelle einen Gesamtüberblick haben muss, denn diese Normen begründen keine *ausschließliche* Kontrollzuständigkeit der jeweiligen Institution. Zudem handelt es sich beim Richtervorbehalt gem. Art. 13 Abs. 3, 4 GG um eine Spezialregelung zur Vorabkontrolle, die laufenden Kontrollen durch

⁴⁰⁹ Vgl. [Teil 2 A. III. 4. b. aa\) \(2\)](#).

⁴¹⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 290, die Ausführungen sind in der Randnummer zur „aufsichtlichen Kontrolle“ enthalten, somit handelt es sich nicht um eine Spezifizierung der Vorabkontrolle.

⁴¹¹ Eine Bund-Länder-Gruppe mit Experten aus dem Bundesinnenministerium, Baden-Württemberg, Bayern, Berlin, Brandenburg, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Sachsen, dem MAD und dem BfV hat den Beschluss der Innenministerkonferenz vorbereitet, vgl.

https://www.stmi.bayern.de/med/aktuell/archiv/2022/220926_verfassungsgerichtsurteil_verfassungsschutz/ (abgerufen am 31.8.2024); *Steinke*, Wie die Bundesregierung den Verfassungsschutz einhegen will.

⁴¹² https://www.imk2022.bayern.de/wp-content/uploads/2022/09/Abschlussbericht_Anlage-3-Unabha%CC%88ngige-Kontrolle.pdf (abgerufen am 31.8.2024), S. 3.

andere Kontrolleure unberührt lässt. Selbst nach der dargelegten Argumentation der B-L-Arbeitsgruppe steht Art.13 Abs. 3, 4 GG mithin einem Gesamtüberblick des für die laufende Kontrolle zuständigen Kontrolleurs nicht entgegen. Darüber hinaus gibt Art. 10 Abs. 2 S. 2 GG nicht vor, dass die G 10-Kommission zuständig ist. Welcher Kontrolleur diese Aufgabe übernimmt, ist offen.⁴¹³

Die Normen verbieten im Übrigen auch nicht, dass die Kontrolleure in die Tätigkeit anderer Kontrolleure Einsicht nehmen.⁴¹⁴ Beispielsweise muss der für die laufende Kontrolle einer eingriffsintensiven Maßnahme zuständige Kontrolleur zwingend die Genehmigung des Vorabkontrolleurs prüfen, um die Rechtmäßigkeit der Durchführung beurteilen zu können. Wenn also der Datenschutzbeauftragte die Datenschutzkonformität einer Maßnahme der strategischen Ausland-Fernmeldeüberwachung prüft, kontrolliert er die Durchführung einer vorab durch das GeKon genehmigten Anordnung. Den Überwachungsgesamtüberblick mit Verweis auf verfassungsimmanent unterschiedliche Zuständigkeiten abzulehnen, kann daher vor dem Hintergrund des komplizierten Zusammenspiels unterschiedlicher Kontrolleure und Kontrollzeitpunkte nicht überzeugen.

Die Nachrichtendienstgesetze müssen deshalb so ausgestaltet sein, dass mindestens einer⁴¹⁵ der Kontrolleure alle Maßnahmen gegenüber einer Person überblicken kann.⁴¹⁶

I. Kontroll-Gesamtüberblick de lege lata

Das Konzept des Kontroll-Gesamtüberblicks ist so neu, dass es – außer in Bayern, Hessen, Sachsen und Hamburg – im geltenden Recht noch nicht mitgedacht worden sein kann. Dennoch hat einer der Rechtskontrolleure auch nach geltendem Recht einen sehr weitreichenden Überblick: der Bundes- bzw. Landesdatenschutzbeauftragte. Der BfDI kann „einen Großteil der Tätigkeiten der Nachrichtendienste des Bundes (...) kontrollieren, liegt doch der überwiegende Teil ihrer Tätigkeiten in der Verarbeitung personenbezogener Daten, also vor allem in der Erhebung und Speicherung, aber auch der Analyse und der Übermittlung an andere Stellen“.⁴¹⁷

⁴¹³ Vgl. [Teil 2 A. III. 3.](#)

⁴¹⁴ Das „in den Blick nehmen“ sei „nicht als überlappende oder mehrfache Zuständigkeit zu verstehen, sondern als Möglichkeit, Einsicht zu nehmen und sich ein umfassendes Bild zu machen“, *Sosna*, GSZ 2022, 245, 251.

⁴¹⁵ *Wetzling/C. Dietrich*, Disproportionate use of commercially and publicly available data, S. 41, betonen, dass dies sowohl für die ex-ante als auch die ex post Kontrolle notwendig ist.

⁴¹⁶ *Bäcker*, Beschwerdeschrift gegen das G 10, S. 66.

⁴¹⁷ *Sosna*, GSZ 2022, 245, 247; zustimmend *Warg*, Recht der Nachrichtendienste, S. 216 Rn. 507; so auch bereits *Riegel*, DöV 1985, 317; *Ruckerbauer*, Stärkung des Datenschutzbeauftragten, S. 7 f.; vgl. zur Kontrollzuständigkeit [Teil 3 D. II. 1.](#)

Beim BfDI handle es sich bei „extensiver Wahrnehmung der Kontrollrechte“ um eine „Super-Fachaufsicht“, die mit dem Hebel des Personenbezugs, den nahezu alle Informationen aufweisen, die bei den Nachrichtendiensten verarbeitet werden, eine umfassende Kontrolle bzw. Steuerung der Aufgabenwahrnehmung vornehmen“ kann. Daher verfüge der BfDI neben der Fachaufsicht und dem PKGr über „die breiteste Zuständigkeits- und Aufgabenspanne aller Kontrollorgane“.⁴¹⁸

1. Zuständigkeitsvorbehalt zugunsten der G 10-Kommission

Bei der Datenschutzkontrolle der Nachrichtendienste wird die Zuständigkeit der Datenschutzbeauftragten auf der Bundesebene und in acht Ländern zugunsten der G 10-Kommissionen eingeschränkt⁴¹⁹. Die Norm auf der Bundesebene wird so ausgelegt, dass der BfDI zwar nicht für die Kontrolle zuständig ist, die Daten aber dennoch zur Kenntnis nehmen darf.⁴²⁰ Hier ändert der Zuständigkeitsvorbehalt zugunsten der G 10-Kommission nichts daran, dass der BfDI einen Gesamtüberblick haben könnte.

Ob die Normen in den Ländern ebenso ausgelegt werden, ist offen. Nur wenn auch die Kenntnisnahme der Daten, für deren Kontrolle die G 10-Kommission zuständig ist, ausgeschlossen wird, wäre es für die jeweiligen LfDI bereits rechtlich unmöglich, einen Gesamtüberblick zu erhalten.

2. Kooperationsnorm

Auf der Bundesebene ist festgelegt, dass die unterschiedlichen Kontrollorgane sich über „allgemeine Angelegenheiten“ ihrer Kontrolltätigkeit austauschen.⁴²¹ Diese Kooperationsnorm bedingt jedoch keinen Kontroll-Gesamtüberblick, denn von ihr ist der Austausch über konkrete Datenverarbeitungen, um den es beim Kontroll-Gesamtüberblick geht, gerade nicht erfasst.

II. Zwischenergebnis

In acht Bundesländern und auf der Bundesebene könnte der Datenschutzbeauftragte bereits de lege lata potenziell alle Datenverarbeitungen des jeweiligen Nachrichtendienstes in den Blick nehmen. In weiteren acht Bundesländern kommt es darauf an, wie der Zuständigkeitsvorbehalt zugunsten der G 10-Kommission ausgelegt wird.

⁴¹⁸ Warg, *Recht der Nachrichtendienste*, S. 216 Rn. 507.

⁴¹⁹ Vgl. [Teil 3 D. II. 7. b. bb\).](#)

⁴²⁰ Vgl. [Teil 3 D. II. 7. b. bb\).](#)

⁴²¹ § 58 Abs. 3 BNDG.

G. Fazit: Defizite der einfach-rechtlichen Ausgestaltung

Die Vorgaben des einfachen Rechts, die mit höherrangigem Recht nicht vereinbar sind, lassen sich wie folgt zusammenfassen:

1. Unabhängige Vorabkontrollen sind bisher nicht für alle eingriffsintensiven Maßnahmen eingeführt worden. Für längerfristige Observationen, den Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern und die Nutzung eines IMSI/IMEI-Catchers muss in vielen Gesetzen noch ein Genehmigungsvorbehalt ergänzt werden.⁴²²
2. Vorab genehmigte Eilanordnungen sind konventionswidrig, wenn die Genehmigung der G 10-Kommission nicht oder zu spät nachgeholt wird.⁴²³
3. Dass die Mitglieder der G 10-Kommissionen uneingeschränkt wiedergewählt werden können, beeinträchtigt ihre Unabhängigkeit und führt zur Verfassungswidrigkeit.⁴²⁴
4. Eine rein ehrenamtliche Tätigkeit der Mitglieder der G 10-Kommissionen kann der verfassungsrechtlichen Anforderung der Wirksamkeit der Kontrolle nicht gerecht werden.⁴²⁵
5. Nicht alle G 10-Kommissionen verfügen über die verfassungsrechtlich „notwendige“ Personal- und Sachausstattung.⁴²⁶
6. Die Vorabkontrolle des UKRats ist insoweit konventionswidrig, als dass sie keine unabhängige Vorabkontrolle der Selektoren bzw. zumindest von Kategorien von Selektoren vorsieht, sondern lediglich eine ex post-Kontrolle durch das AdKon etabliert.⁴²⁷
7. Da die Selektoren für die gezielte Datenerhebung in der Anordnung nicht benannt werden müssen, kann das GeKon diese Suchbegriffe nicht kontrollieren, was verfassungswidrig ist.⁴²⁸
8. Die Protokollierungspflichten des BND sind in konventions- und verfassungswidriger Weise unzureichend.⁴²⁹
9. Dass der UKRat für die Einsichtnahme in Original-Akten ein berechtigtes Interesse geltend machen muss, ist mit der Rechtsprechung des Bundesverfassungsgerichts nicht vereinbar.⁴³⁰

⁴²² Vgl. [Teil 3 A. II.](#)

⁴²³ Vgl. [Teil 3 B. II. 1. b.](#)

⁴²⁴ Vgl. [Teil 3 B. IV. 2. c.](#)

⁴²⁵ Vgl. [Teil 3 B. IV. 3.](#)

⁴²⁶ Vgl. [Teil 3 B. X. 2. a.](#)

⁴²⁷ Vgl. [Teil 3 C. II. 1. a. aa\) \(2\).](#)

⁴²⁸ Vgl. [Teil 3 C. II. 1. a. bb\) \(2\).](#)

⁴²⁹ Vgl. [Teil 3 C. II. 2. c.](#)

⁴³⁰ Vgl. [Teil 3 C. VIII. 2. a.](#)

10. Um die verfassungsrechtlichen Vorgaben zu erfüllen, müsste gesetzlich geregelt werden, dass das AdKon unter anderem aus Personen mit „informationstechnischen Kenntnissen“ bestehen muss.⁴³¹
11. Insoweit die Third Party Rule für den UKRat wie eine Kontrollbarriere wirkt, weil der Zugang zu informationstechnischen Systemen bzw. der Zugang zu Diensträumen mangels alleiniger Verfügungsberechtigung des BND verwehrt wird, ist die Rechtslage verfassungswidrig.⁴³²
12. In Mecklenburg-Vorpommern existiert keine Norm, die die Zuständigkeit des LfDI für die Datenschutzkontrolle beim Verfassungsschutz festlegt. Das ist verfassungswidrig.⁴³³ Selbst wenn man annimmt, die Zuständigkeit sei herleitbar, ist zumindest verfassungswidrig, dass der LfDI weder über Kontrollmittel zur Informationsgewinnung noch über Kontrollergebnissefolgen verfügt.⁴³⁴
13. In vielen Ländern ist für die Datenschutzkontrolle der Verfassungsschutzbehörden keine ausreichende Stellenanzahl vorgesehen, die ihnen „regelmäßige“ Kontrollen ermöglichen würden. Das ist verfassungswidrig.⁴³⁵
14. Die Beanstandung ist keine „wirksame Befugnis“ im Sinne der Rechtsprechung. Alle Fachgesetze, in denen die Beanstandung die effektivste Kontrollergebnisfolge ist, sind daher verfassungswidrig. Soweit die nachrichtendienstliche Tätigkeit in den Anwendungsbereich des Unionsrechts fällt, ist die Ausstattung mit dem unverbindlichen Beanstandungsrecht zusätzlich unionsrechtswidrig.⁴³⁶
15. Der in acht Gesetzen vorgesehene vollständige Ausschluss der Kontrollrechte der Datenschutzbeauftragten ist verfassungswidrig.⁴³⁷
16. Die Verfassungsschutzgesetze von Berlin und Mecklenburg-Vorpommern enthalten kein Kernbereichsschutzkonzept und sind daher offensichtlich verfassungswidrig.⁴³⁸
17. Das Verfassungsschutzgesetz von Sachsen-Anhalt sieht auf der Auswertungsebene keine Sichtung durch eine unabhängige Stelle vor, obwohl es zur Wohnraumüberwachung ermächtigt. Das ist verfassungswidrig. Dass das Verfas-

⁴³¹ Vgl. [Teil 3 C. X.](#)

⁴³² Vgl. [Teil 3 C. XII.](#)

⁴³³ Vgl. [Teil 3 D. II. 1. b.](#)

⁴³⁴ Vgl. [Teil 3 D. II. 5. e.](#)

⁴³⁵ Vgl. [Teil 3 D. II. 4. a. bb\)](#), [Teil 3 D. II. 7. a.](#)

⁴³⁶ Vgl. [Teil 3 D. II. 6. c.](#)

⁴³⁷ Vgl. [Teil 3 D. II. 7. b.](#)

⁴³⁸ Vgl. [Teil 3 E.](#)

sungsschutzgesetz von Schleswig-Holstein beim Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten auch in Zweifelsfällen keine Kontrolle vorsieht, macht das Kernbereichsschutzkonzept verfassungswidrig.⁴³⁹

18. Sechs Verfassungsschutzgesetze sehen zwar eine Sichtung vor, die Stelle ist dort jedoch nicht unabhängig vom Nachrichtendienst. Das ist verfassungswidrig.⁴⁴⁰
19. Die Rechtslage auf der Bundesebene, in Baden-Württemberg und Bremen ist insoweit verfassungswidrig, dass eine unabhängige Sichtung bei kernbereichsrelevanten Daten aus der Wohnraumüberwachung nicht vorgesehen ist, obwohl diese Nachrichtendienste dazu befugt sind.⁴⁴¹
20. Die Regelungen in Brandenburg, Rheinland-Pfalz und dem Saarland, die eine Vorlage nur für Zweifelsfälle vorsehen, sind verfassungswidrig.⁴⁴² Dass auch für Eingriffe in informationstechnische Systeme von Ausländern im Ausland nur eine Sichtung in Zweifelsfällen vorgesehen ist, ist verfassungswidrig.⁴⁴³

⁴³⁹ Vgl. [Teil 3 E. I. 1.](#)

⁴⁴⁰ Vgl. [Teil 3 E. I. 2.](#)

⁴⁴¹ Vgl. [Teil 3 E. III. 1.](#)

⁴⁴² Vgl. [Teil 3 E. III. 1.](#)

⁴⁴³ Vgl. [Teil 3 E. III. 2.](#)

Teil 4

Reformvorschlag für die externe Rechtskontrolle der Nachrichtendienste

„Die rechtliche Absicherung und Einbegung der Nachrichtendienste wird jedoch ein ‘work in progress’ bleiben, das vor allem auch im Dialog aller Beteiligten stetig weiter vorangetrieben werden muss. Entscheidend ist, dass dieser Dialog von einem gemeinsamen Willen zum Recht und zur Verfassung getragen bleibt.“

Prof. Mathias Hong, 2019¹

In diesem Abschnitt wird ein verfassungs- und konventionskonformes Kontrolldesign vorgestellt, das im Rahmen der anstehenden Reformen im Nachrichtendienstrecht als Diskussionshilfe dienen kann. Dazu wird zunächst der Reformbedarf erläutert (A.) und anschließend das Konzept beschrieben (B.).

A. Reformbedarf

Inwieweit das geltende Recht mit den höherrangigen Vorgaben vereinbar ist, wurde bereits untersucht. Die Unvereinbarkeiten mit höherrangigem Recht aufzulösen, ist der zentrale Grund für eine Reform der Rechtskontrolle. Die Vereinbarkeit mit höherrangigem Recht stellt jedoch nur einen Mindeststandard dar, den das einfache Recht zu erfüllen *hat*. Auf diesem Mindeststandard aufbauend können Normen geschaffen werden, mit denen Probleme gelöst werden, die durch die aktuelle Ausgestaltung entstanden sind. Die bestehenden Probleme wurden seit Jahren vielfach artikuliert.

I. Vielzahl der Kontrolleure

Die häufigste Kritik, die von unterschiedlichen Akteuren wie beispielsweise Vertretern der Nachrichtendienste und Wissenschaftlern gleichermaßen geäußert wird, betrifft

¹ Hong, Einsatz von V-Leuten und verdeckten Mitarbeitern, 45, 46.

die als zu hoch empfundene Anzahl an Kontrolleuren und deren zum Teil unzureichend abgegrenzte Kontrollkompetenzen. Die Vehemenz der Kritik lässt sich durch folgende Zitate veranschaulichen:

- „Schindler moniert: ‚Wie die Erfahrung zeigt, intensivieren diese Parallelstrukturen gerade nicht die Kontrolle, sondern machen sie unsystematisch und unübersichtlich.‘ Denn ‚entweder befassen sich mehr oder weniger alle Kontrollinstanzen mit dem gleichen Thema oder man verlässt sich gegenseitig aufeinander mit entsprechendem Erfolg.‘“²
- „‚Wenn die Entwicklung der Rechtsprechung und so manches politisches Projekt im Bereich Verfassungsschutz so weitergehen, dann haben wir bald mehr Kontrolleure als eigentliche Beschaffer und Auswerter, die Informationen über Bestrebungen gegen die Freiheitlich Demokratische Grundordnung aufklären.‘“³
- „Diese Mannigfaltigkeit an Instanzen ist für eine effektive Kontrolle der Geheimdienste nicht förderlich.“⁴
- „Langfristig sollte der Gesetzgeber (...) überlegen, ob der Flickenteppich deutscher Kontrollgremien in eine ganzheitliche und überschaubare Struktur überführt werden könnte.“⁵
- „Bedeutet also die Vielfalt der Kontrollinstanzen und -verfahren ein Mehr an Kontrolle? Oder bedeutet sie umgekehrt ein Mehr an Möglichkeiten, die Tätigkeit der Dienste Kontrollmechanismen zu entziehen und im gepflegten Halbdunkel interner Zirkel zu belassen? Auffällig ist jedenfalls: Die Kontrollinstanzen arbeiten unabhängig voneinander und nebeneinander her. Die eine erfährt nicht, was die andere ermittelt hat und was sie daraufhin veranlasste.“⁶

² So zitiert Ronen Steinke den ehemaligen BND-Präsidenten Schindler in einem Interview vom 22.9.2016, *Steinke*, Früherer BND-Chef kritisiert Kontrollsystem des deutschen Geheimdiensts.

³ Den Präsidenten des Landesamts für Verfassungsschutzes Thüringen, Stephan Kramer, zitierend, *Huesmann*, Der Verfassungsschutz steht vor einer Reform.

⁴ *Marxsen*, DöV 2018, 218, 228.

⁵ *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 17; Prof. Waldhoff zitierend, *Bantlin*, DVBl 2018, 925, 926; vgl. auch *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15, der von „teils disparate[n], zerfaserte[n] und unübersichtliche[n] Kontrollstrukturen“ spricht; ähnlich *Löffelmann*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 21; *Bäcker*, Beschwerdeschrift BNDG, S. 86; *Barczak*, KritV 2021, 91, 127; *Knaust*, Matrix einer neuen Generation auslandsnachrichtendienstlicher Überwachungstätigkeit, S. 561.

⁶ *Gusy*, VerwArch 2015, 437, 443, wobei sich seit 2015 nichts Wesentliches daran geändert hat; ähnlich *Gusy*, Grundrechte und Verfassungsschutz, S. 133; auf diese Gefahr weist auch die Venedig-Kommission hin: „A coherent overall system must be found, bearing in mind that several half remedies or half controls

- „Eine weitere bisher ungeklärte Frage, die von mehreren Gesprächspartnern hervorgehoben wurde, betrifft die unzureichende Koordinierung und die tatsächliche Konkurrenz der unterschiedlichen Aufsichtsgremien, insbesondere zwischen der G 10-Kommission und der Bundesbeauftragten für Datenschutz. Die Aufsicht über die deutschen Nachrichten- und Sicherheitsdienste scheint sehr fragmentiert zu sein, da kein Kontrollgremium eine allgemeine Übersicht über alle Überwachungstätigkeiten hat.“⁷
- „Hier dürften sowohl bei Anordnung und Vorabprüfung entsprechender Erhebungsmaßnahmen wie auch im Zuge der Kontrolle der Rechtmäßigkeit der Weiterverarbeitung der gewonnenen Daten notwendigerweise Doppelstrukturen und Überschneidungen entstehen.“⁸
- „Diese ausufernde Kontrollbürokratie ist die Schwester der Ineffizienz.“⁹

Eine Konsequenz der großen Anzahl an externen Kontrolleuren ist, dass es auf der internationalen Ebene nicht den einen Ansprechpartner für die Nachrichtendienstkontrolle in Deutschland gibt, was „die strukturierte Beteiligung deutscher Aufsichtsbehörden“ ausbremst.¹⁰

II. Aufwand für die Kontrollierten

Die Anzahl an Kontrolleuren wirkt sich auf die Kontrollierten aus: Je mehr Kontrolleure existieren, desto höher ist der Aufwand auf Seiten der Nachrichtendienste. Insofern muss beachtet werden, dass die Tätigkeit des Kontrollierten durch die Kontrolle nicht über Gebühr behindert werden sollte.¹¹

Dabei ist es nicht zwingend die Menge der Kontrollanfragen unterschiedlicher Kontrolleure, die den Aufwand erhöhen, denn es ist denkbar, dass ein Kontrolleur ebenso viele Anfragen stellt wie mehrere andere. Vielmehr entsteht die vermeidbare, zusätzliche Arbeit dadurch, dass Mitarbeiter der Nachrichtendienste die unterschiedlichen Rechtsgrundlagen der Kontrolleure beherrschen und ihre Ansprechpartner verwalten müssen. Vor allem kann de lege lata nicht ausgeschlossen werden, dass unterschiedliche

can be worse than none, as there is the risk that each control/remedies system could refrain from acting on the assumption that the other is doing the work.“, *Venedig-Kommission*, Report 2015, S. 58 Rn. 269.

⁷ *Muižnieks*, Bericht des Menschenrechtskommissars des Europarats, S. 19 Rn. 61.

⁸ *Steiner*, GSZ 2023, 124, 127 zu „doppelrelevanten Aufklärungsanliegen“ nach G 10 und BNDG.

⁹ *Hanning/Schindler*, Gastbeitrag.

¹⁰ *Wetzling*, Gastkommentar; *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 11.

¹¹ „Er sei nicht ‚gegen eine sinnvolle weitere Kontrolle‘, sagte Kramer. ‘Sie muss aber so ausgestaltet sein, dass sie die Rechtmäßigkeit unserer Maßnahmen prüft und gleichzeitig unsere Arbeit nicht unnötig verzögert oder gar behindert‘, den Präsidenten des LfV Thüringen, Stephan Kramer, zitierend, *Huesmann*, Der Verfassungsschutz steht vor einer Reform; *Löffelmann*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 21.

Kontrolleure Gleiches kontrollieren, womit sich das Verhältnis von Aufwand und Nutzen der Kontrollen umkehrt.

Angesichts der großen sicherheitspolitischen Herausforderungen sollte die Anzahl der Kontrolleure verringert werden. Darüber hinaus sollten es die rechtlichen Grundlagen den verbleibenden Kontrolleuren ermöglichen, ihre Arbeit besser koordinieren zu können.¹²

III. Hohe Komplexität

Das Recht der Nachrichtendienste ist komplex und nur schwer verständlich.¹³ Die Normen über die Rechtskontrolle der Nachrichtendienste bilden hiervon – leider – keine Ausnahme. Auch sie sind verteilt über unterschiedliche Gesetze und verweisen (gesetzesübergreifend) aufeinander. Hinzu kommt, dass die Kontrollmittel und Kontrollergebnisse der unterschiedlichen Kontrolleure sich deutlich voneinander unterscheiden.¹⁴ Das ist vor allem für die Praxis, aber auch für den Gesetzgeber und die Wissenschaft kein wünschenswerter Zustand.

Daher wird zu Recht gefordert, dass das Nachrichtendienstrecht insgesamt verständlicher ausgestaltet werden muss.¹⁵

IV. Mangel an Ressourcen

Darüber hinaus wird häufig kritisiert, dass den Kontrolleuren keine ausreichenden Ressourcen zur Verfügung stehen.¹⁶ Jedenfalls gegenüber dem gut ausgestatteten UKRat überzeugt dieser Vorwurf seit der letzten Reform nicht mehr. Auf der Landesebene greift die Kritik jedoch nach wie vor. Dies betrifft beispielsweise die elf Bundesländer, in denen der G 10-Kommission keine Mitarbeiter mit technischem Sachverstand zur Verfügung zu stellen sind.¹⁷ Denn neben der ausreichenden Personalausstattung ist es

¹² Vgl. [Teil 4 B. I. 5. b.](#)

¹³ *Löffelmann/Zöller*, Nachrichtendienstrecht, S. 5; *Gärditz*, GSZ 2021, 905, 914.

¹⁴ Zum BND: *Löffelmann*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 21.

¹⁵ U.a. *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 23 f.; vgl. auch „Bereinigung des Nachrichtendienstrechts“ bei *Barczak*, KritV 2021, 91, 96.

¹⁶ „The Commissioner is particularly concerned by the lack of resources and technical expertise of the oversight bodies and their secretariat“, *Muižnieks*, Bericht des Menschenrechtskommissars des Europarats, S. 16 Rn. 58; Der ehemalige BND-Präsidenten Schindler in einem Interview vom 22.9.2016, *Steinke*, Früherer BND-Chef kritisiert Kontrollsystem des deutschen Geheimdiensts 2016; *Marxsen*, DöV 2018, 218, 228.

¹⁷ Vgl. [Teil 3 B. X. 2. c.](#): Eine solche gesetzliche Verpflichtung fehlt in Bayern, Baden-Württemberg, dem Saarland, Hessen, Niedersachsen, Hamburg, Bremen, Schleswig-Holstein, Brandenburg, Thüringen, Sachsen.

besonders wichtig, dass den Kontrolleuren technische Expertise für die Nachvollziehbarkeit der Datenverarbeitungen zur Verfügung steht.¹⁸

V. Staatswohl- Einrede

Die Kontrollbegehren vieler Datenschutzbeauftragter können de lege lata mit Verweis auf das Staatswohl verweigert werden.¹⁹ Da Kontrollen Kenntnis über den Ist-Zustand voraussetzen, beeinträchtigt dies ihre Wirksamkeit. Das ist aus zwei Gründen nicht hinnehmbar: Erstens werden die Kontrolleure bei den Datenschutzbeauftragten sicherheitsüberprüft. Zweitens dürfen Kontrollbegehren der G 10-Kommissionen und des UKRats nicht verweigert werden. Die Kontrollbegehren der Datenschutzbeauftragten insoweit schlechter zu stellen, ist deshalb nicht überzeugend. Das gilt umso mehr, als die Datenschutzbeauftragten nach geltendem Recht am ehesten den vom Bundesverfassungsgericht geforderten Kontrollgesamtüberblick gewährleisten können.

B. Eckpunkte für einen Reformvorschlag

Ein optimales Kontrolldesign müsste einerseits die höherrangigen Vorgaben beachten und andererseits die Probleme des aktuellen Kontrolldesigns²⁰ auflösen. Für die Bundes- und Landesebene bieten sich unterschiedliche Lösungen an, die gesondert erörtert werden.

I. Reform der externen Rechtskontrolle auf der Bundesebene

Auf der Bundesebene müsste eine klare Kompetenzzuweisung erfolgen. Dem GeKon sollte die Vorabkontrolle aller eingriffsintensiven, nachrichtendienstlichen Befugnisse und dem BfDI die laufende und nachträgliche Rechtmäßigkeitskontrolle übertragen werden. Die G 10-Kommission und das AdKon sollten aufgelöst werden (1.). Das GeKon sollte als unabhängige Stelle zum Kernbereichsschutz eingesetzt werden (2.). Außerdem müssen die Defizite bei den Rechtsgrundlagen der Kontrolle behoben werden (3., 4.). Der BfDI erhält damit einen Kontrollgesamtüberblick (5.). Ihm sollte die Aufgabe übertragen werden, stellvertretend für alle deutschen Nachrichtendienstkontrolleure als internationaler Ansprechpartner zu agieren (6.). Um etwaige Kontrolllücken

¹⁸ Sven Meyer-Ottens, Technischer Direktor beim BND, auf dem 2. Symposium zum Recht der Nachrichtendienste am 15. und 16.3.2018 in Berlin, *Schönfeldt*, JZ 2018, 927, 928; BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 284 f.

¹⁹ Vgl. [Teil 3 D. II. 7. b.](#)

²⁰ Vgl. [Teil 4. A.](#)

schließen zu können, ist ein enger Austausch zwischen den Kontrolleuren und dem Gesetzgeber notwendig, um die Gesetze gegebenenfalls anpassen zu können (7.).

1. Vereinfachtes Kontrolldesign

Das Kontrolldesign lässt sich vereinfachen, indem die Kontrollen nur noch durch das GeKon und den BfDI erfolgen. Die Aufgaben der G 10-Kommission sollen dabei dem GeKon, die des AdKon dem BfDI übertragen werden. Dadurch lässt sich zum einen die Zahl der Kontrolleure um zwei reduzieren, zum anderen werden vorhandene Doppelzuständigkeiten aufgelöst.

a. Zentralisierung der Vorabkontrolle beim GeKon

Das gerichtsähnliche Kontrollgremium des UKRats sollte zukünftig für die Vorabkontrolle aller eingriffsintensiven Maßnahmen der Nachrichtendienste des Bundes zuständig sein.²¹ Es würde dann nicht mehr nur einen Teil der Tätigkeit des BND, sondern alle eingriffsintensiven Tätigkeiten des BND, des BfV und des MAD genehmigen. Seine Aufgaben würden damit massiv ausgeweitet. Dies ist verfassungsrechtlich zwar keineswegs zwingend, empfiehlt sich aber aus unterschiedlichen organisatorisch-praktischen Gründen: Zunächst verfügt der UKRat bereits heute über ein hohes Budget und viele Stellen.²² Zudem sind seine Rechtsgrundlagen weitgehend verfassungskonform ausgestaltet worden²³, sodass mit vergleichsweise geringen gesetzlichen Anpassungen ein überzeugendes Vorabkontrollinstrument zur Verfügung stehen würde.

Die vielfach geäußerten Bedenken dahingehend, dass mit einer Aufgabenerweiterung des UKRats eine Schwächung des PKGr verbunden wäre²⁴, sind nicht stichhaltig, weil es sich bei der politischen Kontrolle um ein Aliud zur Rechtskontrolle handelt, was eine Aufrechnung und Konkurrenz beider Kontrollarten unmöglich macht²⁵.

²¹ *Warg*, Recht der Nachrichtendienste, S. 217 Rn. 508; als naheliegend beurteilt von *Gärditz*, Verfassungsblog vom 2.5.2022; *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 2; *Wetzling*, Bedingt kontrollfähig, S. 19.

²² *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 14.

²³ Vgl. [Teil 3 C.](#)

²⁴ Diese Befürchtung wird vor allem von Seiten der Parlamentarier geäußert, <https://www.sueddeutsche.de/politik/bnd-verfassungsschutz-kontrolle-ueberwachung-1.5745432?reduced=true> (abgerufen am 31.8.2024).

²⁵ Vgl. [Teil 1 A. I. 2.](#)

b. Datenschutzkontrolle durch den BfDI und Auflösung des AdKon

Zukünftig sollten für die laufenden und nachträglichen Kontrollen ausschließlich der BfDI zuständig sein.²⁶

Bereits vor der Verabschiedung der gesetzlichen Grundlagen des UKRats wiesen mehrere Experten darauf hin, dass sich die Zuständigkeiten von AdKon und BfDI nach dem geplanten Gesetz überschneiden werden.²⁷ Man empfahl dem Gesetzgeber, die Zuständigkeit des BfDI insoweit zu begrenzen²⁸ oder detailliertere Vorschriften zu entwerfen, in denen die Zusammenarbeit der unterschiedlichen Kontrolleure besser abgestimmt wird.²⁹ Bedauerlicherweise wurde keiner dieser Vorschläge umgesetzt.

Nach geltendem Recht sind daher sowohl der BfDI als auch das AdKon für die Kontrolle von Datenverarbeitungen im Rahmen der strategischen Ausland-Fernmeldeaufklärung und für Online-Durchsuchungen von Ausländern im Ausland zuständig.³⁰ Dieser Zustand ist untragbar, weil sich durch die Doppelzuständigkeit der Aufwand für die Nachrichtendienste erhöht, ohne dass damit ein rechtsstaatlicher Gewinn verbunden wäre. Zumal unterschiedlichste Experten fordern, dass die Anzahl der Kontrolleure dringend zu reduzieren ist.³¹ Es spricht vieles dafür, diese Parallelzuständigkeit zugunsten des BfDI aufzulösen.³² Denn wenn man den BfDI für allein zuständig erklärt, kann das AdKon mangels anderer Zuständigkeiten aufgelöst werden.

aa) Zuständigkeit des BfDI für sonstige Datenschutzkontrollen der Nachrichtendienste

Das AdKon hat nach geltendem Recht ohnehin eine sehr eng umgrenzte Zuständigkeit, denn seine Kontrolltätigkeit ist auf die Kontrolle der strategischen Ausland-Aufklärung und Eingriffe in informationstechnische Systeme von Ausländern im Ausland beschränkt.³³ Demgegenüber kontrolliert der BfDI bereits jetzt die Rechtmäßigkeit nahezu³⁴ aller anderen nachrichtendienstlichen Tätigkeiten. Dementsprechend verfügt

²⁶ So bereits *Wetzling/Moßbrucker*, BND-Reform, die Zweite, S. 15 f.

²⁷ *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 25; *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15.

²⁸ *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 25.

²⁹ *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15.

³⁰ Vgl. [Teil 3 D. III.](#); *Löffelmann/Zöller*, Nachrichtendienstrecht, S. 263; *Sosna*, GSZ 2022, 245, 250.

³¹ Vgl. [Teil 4 A. I.](#)

³² Für eine Übertragung dieser Aufgabe auf den BfDI bereits *Wetzling/Moßbrucker*, BND-Reform, die Zweite, S. 7; *Markard*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 9; *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 531; *Bäcker*, Beschwerdeschrift G 10, S. 67.

³³ Vgl. [Teil 3 C. II. 2.](#)

³⁴ De lege lata besteht noch ein Zuständigkeitsvorbehalt zugunsten der G 10-Kommission. Die G 10-Kommission sollte jedoch aufgelöst werden, s.u. [Teil 4 B. I. 1. c.](#)

der BfDI über eine breite Expertise und Erfahrung.³⁵ Insgesamt arbeiten dort momentan 29 Fachleute³⁶ im Bereich der Nachrichtendienstkontrolle, unter anderem im „Referat 34“ mit Zuständigkeit für den Bundesnachrichtendienst, das Militärische Nachrichtenwesen und den UKRat.

bb) Vermeidung von Interessenskonflikten bei Kontrolle des AdKon

Gegen eine Alleinzuständigkeit des UKRats für die gesamte Rechtskontrolle spricht zudem folgende Überlegung des EGMR: Er weist in der Entscheidung „Centrum for Rättvisa vs. Sweden“ (2021) darauf hin, dass ein Kontrolleur, der selbst für die Kontrollen auf mehreren Stufen (Vorabkontrolle, Kontrolle während der Durchführung sowie nachträgliche Kontrolle) zuständig ist – im schwedischen Beispiel auch für die nachträgliche Kontrolle – in Situationen geraten wird, in denen er die Rechtmäßigkeit seiner eigenen Entscheidung zu prüfen hat und ein Interessenkonflikt entstehen kann, aus dem die Versuchung erwachsen könnte, über eigene Fehlentscheidungen hinwegzusehen.³⁷ Sowohl das AdKon als auch das GeKon sind Teil des UKRats. Das AdKon wird (zumindest indirekt) die Rechtmäßigkeit der Genehmigung des GeKon zu prüfen haben. Um den beschriebenen Interessenkonflikt zu vermeiden, bietet es sich an, die Zuständigkeit für die laufende und nachträgliche Kontrolle stattdessen allein dem BfDI zu übertragen. Außerdem kann die Kontrolle durch eine weitere unabhängige Stelle der Gefahr einer Fraternisierung zwischen Vorabkontrolleur und Nachrichtendienst vorbeugen³⁸.

³⁵ Markard, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 9; Vogt, Strategische Auslandsstelekkommunikationsüberwachung, S. 531; insoweit Riegel schon 1985: „Die für den Sicherheitsbereich zuständigen Mitarbeiter des Bundesbeauftragten für den Datenschutz haben durch langjährige Prüfungen einen – auf die Datenverarbeitung beschränkten – Überblick und ein Querschnittswissen, das kaum in einer anderen Kontrollinstitution, sei es ein Gericht, sei es die Parlamentarische Kontrollkommission, sei es die G-10-Kommission, in diesem Ausmaß vorhanden ist“, Riegel, DöV 1985, 317.

³⁶ Vgl. [Teil 3 D. II. 4. a. aa.](#)

³⁷ Vgl. [Teil 2 B. I. 4. b. ff.](#), EGMR 25.5.2021– 35252/08 Rn. 359, 360, 364 – Centrum för Rättvisa gg. Schweden.

³⁸ Wegen dieser Gefahr sprach sich Friesenhahn bereits 1981 gegen einen Genehmigungsvorbehalt aus: „Die Regierung muß ihr bzw. ihrer nachgeordneten Dienststellen Handeln verantworten und vor dem Kontrollorgan rechtfertigen. Würde das Kontrollorgan gemeinsam mit der Regierung exekutivisch tätig werden – etwa indem eine Maßnahme *vorher* von dem Kontrollgremium genehmigt werden muß, so würde sich die Kontrolle in Mitregierung verwandeln“, Friesenhahn, Kontrolle, 87, 98.

cc) Kontroll-Gesamtüberblick

Vor allem spricht für eine alleinige Zuständigkeit des BfDI, dass er als einziger Kontrolleur bereits nach geltendem Recht über einen potenziellen Gesamtüberblick verfügt.³⁹ Übertrüge man die laufende und nachträgliche Kontrolle stattdessen allein dem AdKon, würde der potenzielle Gesamtüberblick des BfDI über alle nachrichtendienstlichen Datenverarbeitungen hingegen stark beschränkt. Speziell der Gesamtüberblick ist jedoch der wichtigste Vorteil der Rechtskontrollen des BfDI. Das lässt sich an einem aktuellen Beispiel gut illustrieren: Im Berichtsjahr 2023 hat der BfDI erstmalig das Gemeinsame Terrorabwehrzentrum von Bund und Ländern kontrolliert, in dem sich unter anderem die Nachrichtendienste und das Bundeskriminalamt austauschen. Der BfDI konnte für diese Kontrolle ein Team aus den Referaten zur Kontrolle des BND, des BfV und des Bundeskriminalamts zusammenstellen.⁴⁰ Kein anderer Rechtskontrolleur verfügt über eine so breite Expertise und Zuständigkeit. Gerade weil die Kontrollierten behördenübergreifend kooperieren, ist die behördenübergreifende Zuständigkeit des BfDI für die Wirksamkeit der Rechtskontrolle so wertvoll.⁴¹

dd) Keine unbehebbarsten Nachteile

Demgegenüber können die Einwände, die gegen eine Beauftragung des BfDI geltend gemacht wurden, entkräftet werden.

(1) Third Party Rule-Einwand

Für eine Beauftragung des AdKon statt dem BfDI wurde angeführt, dass der Kontrolle des BfDI die Third Party Rule entgegengehalten werden kann.⁴² Dem ist in Bezug auf die aktuelle Rechtslage zuzustimmen.⁴³ Dass die Kontrollmittel des BfDI (im Gegensatz zu denen der G 10-Kommission und des UKRat) aus Staatswohlgründen außer Kraft gesetzt werden können, war jedoch noch nie überzeugend und sollte deshalb zukünftig

³⁹ Vgl. [Teil 3 F. I.](#), vgl. auch *Riegel*, DöV 1985, 317.

⁴⁰ [32. Tätigkeitsbericht des BfDI](#) 2023, S. 126.

⁴¹ So bereits *Riegel* 1985: „Damit fehlt [Anm.: der G 10-Kommission im Unterschied zum BfDI] sowohl der Überblick über die Zusammenhänge nicht nur der Nachrichtendienste untereinander (und nur diese werden selbst von der umfassender zuständigen Parlamentarischen Kontrollkommission geprüft), sondern insbesondere auch für die vielfältigen Querverbindungen zwischen Polizeien des Bundes und der Länder und den Nachrichtendiensten zu anderen Behörden.“, *Riegel*, DöV 1985, 317; vgl. auch BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 216.

⁴² *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 25.

⁴³ Vgl. [Teil 3 D. II. 7. b. aa.](#)

nicht mehr vorgesehen sein.⁴⁴ Mit dem Third Party Rule-Einwand gegen eine Zuständigkeit des BfDI zu argumentieren, kann in dem hier vorgeschlagenen Kontrolldesign daher nicht überzeugen.

(2) Höheres Rechtsschutzniveau

Darüber hinaus wird betont, dass über das AdKon „ein höheres Rechtsschutzniveau“ zu erreichen sei, weil es über die „Eskalationsmöglichkeit“ verfügt, dem GeKon Beanstandungen zur verbindlichen Entscheidung vorzulegen.⁴⁵ Dieser Einwand überzeugt zumindest mit Blick auf das geltende Recht, da dem BfDI nur ein Beanstandungsrecht zusteht.⁴⁶

Da aber das Beanstandungsrecht ohnehin keine „wirksame Befugnis“ im Sinne der Rechtsprechung des Bundesverfassungsgerichts ist, müssen die Kontrollergebnisse des BfDI sowieso gestärkt werden.⁴⁷ Damit entfiele auch der vorgebrachte Einwand gegen eine Kontrollzuständigkeit des BfDI nicht.

(3) Lähmung der Datenschutzaufsicht

Schließlich wird gegen eine Übertragung dieser Aufgabe auf den BfDI geltend gemacht, dies würde ihn „dysfunktional in die dem Geheimschutz unterliegenden Mechaniken der Nachrichtendienstverwaltung hineinziehen, was dann eine Lähmung der eben auch politischen und der Öffentlichkeit zugewandten Datenschutzaufsicht zur Folge hätte.“⁴⁸ Dem ist insoweit zuzustimmen, dass die mit strengen Geheimhaltungserfordernissen verbundene Rechtskontrolle nachrichtendienstlicher Datenverarbeitungen mit der sonstigen Kontrolltätigkeit des BfDI nicht vergleichbar ist. Beispielsweise kann der BfDI seine Kontrollergebnisse nicht detailliert in seinem Tätigkeitsbericht veröffentlichen.⁴⁹ Dieser Nachteil wird jedoch an anderer Stelle mit Vorteilen ausgeglichen: unter anderem kann der BfDI sein aus der Kontrolle gewonnenes Wissen im Rahmen von Gesetzgebungsprozessen abstrakt einbringen und auf diese Weise die wegen der Heimlichkeit der nachrichtendienstlichen Arbeit strukturell schlecht informierte Legislative bei der Gesetzgebung mit ihrer praktischen Erfahrung fachlich unterstützen.

⁴⁴ Vgl. [Teil 3 D. II. 7. b. aa. \(2\)](#).

⁴⁵ [Dietrich](#), Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 25; vgl. [Teil 3 C. IX.](#)

[2.](#)

⁴⁶ Vgl. [Teil 3 D. II. 6. a.](#)

⁴⁷ Vgl. [Teil 3 D. II. 6. c.](#)

⁴⁸ [Gärditz](#), Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 11.

⁴⁹ Vgl. insoweit schon [Gusy](#), Richterliche Kontrolle, 67, 90.

Hinzu kommt, dass der BfDI nicht erst dadurch in die durch den Geheimschutz geprägte Nachrichtendienstverwaltung einbezogen worden wäre, sondern er war und ist ohnehin für die Kontrolle aller anderen nachrichtendienstlichen Datenverarbeitungen zuständig.

(4) Verzahnung mit GeKon

Gegen eine Auflösung des AdKon lässt sich zudem anführen, dass das GeKon und das AdKon normativ miteinander verzahnt sind und dass so Synergien entstehen, auf die nicht verzichtet werden sollte. Beispielsweise kann das GeKon dem AdKon konkrete, einzelfallbezogene Prüfaufträge erteilen (§ 52 Abs. 3 BNDG).⁵⁰ Dadurch wird das GeKon befähigt, prüfungsbedürftige Aspekte oder Vorgänge, auf die es im Rahmen seiner Kontrolltätigkeit stößt, näher beleuchten zu lassen. Diese Aufgabe könnte auch der BfDI übernehmen. Dafür müsste die Zusammenarbeitsvorschrift so geändert werden, dass nicht nur ein allgemeiner Austausch, sondern eine Zusammenarbeit, auch in konkreten Fällen, ermöglicht wird (§ 58 Abs. 3 BNDG).⁵¹

Außerdem ist die Expertise des AdKon für das GeKon nützlich, um Entscheidungen vorzubereiten.⁵² Mit der Auflösung des AdKon muss diese Expertise jedoch nicht zwingend verloren gehen. Einige Mitarbeiter könnten dem GeKon zuarbeiten, während andere in die Fachabteilung des BfDI integriert werden.

Im Ergebnis ist es mit entsprechendem gesetzlichem und organisatorischem Gestaltungswillen möglich, die wegen der Auflösung des AdKon verlorengehenden Synergien auszugleichen.

ee) Abgrenzung zum GeKon

In einem so angedachten Kontrolldesign muss geklärt werden, wie die Zuständigkeiten von GeKon und BfDI abgegrenzt werden. Das GeKon ist bereits der Vorabkontrolleur aller Maßnahmen der technischen Aufklärung nach dem BNDG im Ausland. Zukünftig sollte das GeKon darüber hinaus alle anderen eingriffsintensiven nachrichtendienstlichen Tätigkeiten genehmigen. Demgegenüber soll der BfDI für die laufende und nachträgliche Rechtmäßigkeitskontrolle zuständig sein. Im Ergebnis gibt es nach diesem Modell also zwei kompetenzmäßig deutlich abgrenzbare Rechtskontrolleure: das GeKon als ex ante-Kontrolleur und den BfDI als ex post-Kontrolleur.

⁵⁰ Vgl. [Teil 3 C. II. 2. a.](#)

⁵¹ Vgl. [Teil 4 B. I. 5. b.](#), Wetzling/Moßbrucker, BND-Reform, die Zweite, S. 16.

⁵² Dt. Bundestag, Drs. 19/26103, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 111.

(1) Teilzuständigkeit des GeKon für die Datenschutzkontrolle

Zu dieser klaren Zweiteilung passt zunächst nicht, dass de lege lata nicht nur das AdKon, sondern außerdem das GeKon für die laufende Rechtskontrolle zuständig ist. Dessen Zuständigkeit ist allerdings auf vier Bereiche begrenzt (§ 42 Abs. 5 BNDG).⁵³ Sie erstreckt sich erstens auf die Kontrolle von Daten, bei denen sich bei der Verarbeitung herausstellt, dass sie aus Vertraulichkeitsbeziehungen stammen⁵⁴ und zweitens auf die Kontrolle der Zweckänderung von Daten, die ursprünglich zur politischen Unterrichtung verwendet wurden und dann zur Verhinderung einer unmittelbar bevorstehenden Gefahr für besonders wichtige Rechtsgüter übermittelt werden sollen⁵⁵. Darüber hinaus kontrolliert das GeKon drittens die Dienstvorschriften des BND zur technischen und organisatorischen Umsetzung der technischen Aufklärung, „soweit diese Regelungen zur Datenauswertung“ enthalten⁵⁶ und prüft viertens Sachverhalte, die ihm das AdKon zur endgültigen Entscheidung vorlegt, weil einer Beanstandung nicht abgeholfen wurde^{57, 58}.

Nach diesem Modell entfällt die zuletzt genannte Rechtmäßigkeitskontrolle, die durch die Vorlage des AdKon erforderlich wird, weil das AdKon aufgelöst und der BfDI mit einem abschließenden Entscheidungsrecht ausgestattet wird. Die Rechtmäßigkeitskontrolle von Dienstvorschriften der Nachrichtendienste sollte zukünftig ausschließlich der BfDI übernehmen. Damit wird eine Mehrfachbelastung der Nachrichtendienste durch doppelte Kontrollen verhindert. Das GeKon muss Zugang zu diesen Dienstvorschriften haben, um seine Aufgabe der Vorabkontrolle wahrnehmen zu können. Etwaige rechtliche Bedenken zu den Dienstvorschriften sollte das GeKon dann dem BfDI kommunizieren, damit dieser das bei seiner Prüfung berücksichtigen kann. Für die nachträgliche Kontrolle von Daten, bei denen sich nach der Genehmigung erst herausstellt, dass sie aus einer Vertraulichkeitsbeziehung stammen oder dass ihr Zweck geändert werden muss, sollte das GeKon zuständig bleiben. Dafür spricht der enge Zusammenhang zur ursprünglichen Genehmigung, die das GeKon erteilt hat.

Falls diese Kontrollen dennoch dem BfDI übertragen werden, ist eine enge Abstimmung mit dem GeKon zwingend.

⁵³ Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 25.1.2021, S. 104.

⁵⁴ § 42 Abs. 2 Nr. 1, § 23 Abs. 3, § 42 Abs. 4 Nr. 1, § 35 Abs. 3 BNDG.

⁵⁵ § 42 Abs. 2 Nr. 2, § 29 Abs. 7, § 30 Abs. 5 BNDG; § 42 Abs. 4 Nr. 2, § 38 Abs. 7, § 42 Abs. 2 Nr. 2, § 39 Abs. 4 BNDG.

⁵⁶ § 42 Abs. 2 Nr. 3, § 62 BNDG.

⁵⁷ § 42 Abs. 2 Nr. 4 BNDG, § 42 Abs. 4 Nr. 3, § 52 Abs. 3 BNDG.

⁵⁸ Vgl. [Teil 3 C. II. 1.](#)

(2) Abstimmungsbedarf

Das GeKon und der BfDI müssen zukünftig in Einzelfällen zusammenarbeiten können, um Kontrolllücken zu vermeiden. Dafür muss § 58 Abs. 3 BNDG aufgehoben oder angepasst werden, sodass der Austausch nicht auf allgemeine Angelegenheiten begrenzt bleibt. Nur dann kann das GeKon den BfDI beispielsweise darauf hinweisen, dass es eine Anordnung nur unter bestimmten Voraussetzungen genehmigt hat, deren Einhaltung der BfDI sodann stichprobenartig prüfen kann.⁵⁹

c. Auflösung der G 10-Kommission

Da die bisherigen Aufgaben der G 10-Kommission nach diesem Vorschlag durch den UKRat und den BfDI⁶⁰ wahrgenommen werden, besteht für die G 10-Kommission keine Notwendigkeit mehr, sodass sie aufgelöst werden kann.⁶¹ Eine Auflösung dieser Institution wäre verfassungsrechtlich möglich⁶², soweit ihre Aufgabe von einem anderen Kontrolleur übernommen wird. Mit der Auflösung der G 10-Kommission würde der kritisierten Zersplitterung der Kontrolleure entgegengewirkt.⁶³ Die problematischen Überschneidungen der Tätigkeiten von GeKon und G 10-Kommission, auf die das ehemalige Mitglied des GeKon, Steiner, hinweist, würden sich auf diese Weise erledigen.⁶⁴

Die Auflösung der G 10-Kommission wäre verfassungsrechtlich unproblematisch, weil es im Gestaltungsspielraum des Gesetzgebers liegt, wen er mit der Kontrolle betraut. Das enorme Fach- und Erfahrungswissen der G 10-Kommissionsmitglieder sollte jedoch im Rahmen des UKRats eingebunden werden.⁶⁵

Die Kommissionsmitglieder könnten grundsätzlich sowohl im GeKon als auch im AdKon tätig werden. Da aber die administrative Kontrolle des UKRats nach diesem

⁵⁹ Wetzling/Moßbrucker, BND-Reform, die Zweite, S. 16.

⁶⁰ Zur Übertragung der nachträglichen Rechtmäßigkeitskontrolle von der G 10-Kommission auf den BfDI bereits Bächer, Beschwerdeschrift G 10, S. 67.

⁶¹ „Anzustreben ist eine Ablösung der G 10-Kommission. Es ist für eine wirksame Kontrolle, die Geheimhaltung und die Sicherheit kontraproduktiv, an diesem Organ weiter festzuhalten“, so Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15; Dietrich, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 25; Markard, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 9; bereits BT-Drs. 19/26221, Antrag B 90/Die Grünen vom 27.1.2021, S. 7, <https://dserv.bundestag.de/btd/19/262/1926221.pdf> (abgerufen am 31.8.2024); Vogt, Strategische Auslandstelekommunikationsüberwachung, S. 656; Wetzling/Moßbrucker, BND-Reform, die Zweite, S. 19.

⁶² BVerfG, Beschluss v. 20.9.2016 - 2 BvE 5/15 - Rn. 45.

⁶³ Vgl. Teil 4 A. I.

⁶⁴ „Überschneidungsbereiche“ ergäben sich, weil der Katalog von § 5 Abs. 1 S. 2 G 10 sich teilweise mit „Gefahrenbereichen und Schutzgütern“ gem. § 19 Abs. 4 S. 1 BNDG deckt, Steiner, GSZ 2023, 124, 127.

⁶⁵ Wetzling/Vieth, Mehr Rechtskontrolle wagen, S. 18, 22; Vogt, Strategische Auslandstelekommunikationsüberwachung, S. 656.

Vorschlag aufgelöst werden soll, kommt das AdKon nicht in Betracht. Stattdessen sollten die Kommissionsmitglieder in das GeKon integriert werden. Falls zukünftig Betroffenenvertreter in das Verfahren des GeKon eingebunden werden sollen⁶⁶, könnten die Kommissionsmitglieder beispielsweise diese Aufgabe übernehmen. Unter Berücksichtigung ihrer bisherigen Arbeit erscheint es jedoch sinnvoller, die G 10-Kommissionsmitglieder als zusätzliche Richter für das GeKon einzusetzen. Zusätzliche Richter sind erforderlich, da sich der Arbeitsaufwand durch die Zentralisierung der Vorabkontrolle beim GeKon erheblich steigern wird. Um dies zu ermöglichen, müssten jedoch die Vorgaben zur Besetzung des UKRats geändert werden.⁶⁷

2. GeKon als „unabhängige Stelle“ zum Kernbereichsschutz

Zukünftig sollte dem GeKon die Rolle der „unabhängigen Stelle“ für alle verletzungsgeneigten Befugnisse der Nachrichtendienste des Bundes übertragen werden⁶⁸. Bereits de lege lata übernimmt das GeKon diese Aufgabe für Daten aus der strategischen-Ausland-Fernmeldeaufklärung und von Eingriffen in informationstechnische Systeme von Ausländern im Ausland, wenn im Rahmen der Weiterverarbeitung Zweifel über die Kernbereichsrelevanz bestehen und die Daten nicht unverzüglich gelöscht werden sollen.⁶⁹

Da die G 10-Kommission aufgelöst werden soll, ist ihre Zuständigkeit beim Kernbereichsschutz dem GeKon zu übertragen. Darüber hinaus muss auf der Bundesebene eine Regelung zum Kernbereichsschutz bei der Wohnraumüberwachung eingeführt werden, die vorsieht, dass sämtliche Daten zunächst durch eine unabhängige Stelle gesichtet werden.⁷⁰

3. Rechtsgrundlagen für die Kontrolle durch das GeKon

Wenn das GeKon für die Vorabkontrolle aller eingriffsintensiven nachrichtendienstlichen Mittel zuständig ist, ergibt seine gesetzliche Regelung (ausschließlich) im BNDG keinen Sinn mehr. Stattdessen sollte der Auftrag des GeKon in einem separaten Gesetz detailliert werden, für das bereits die Bezeichnung „Kontrollratsgesetz“⁷¹ vorgeschlagen

⁶⁶ Vgl. [Teil 4 B I. 3. b. aa\).](#)

⁶⁷ Vgl. [Teil 4 B I. 3. b. cc\).](#)

⁶⁸ Vgl. [Teil 2 A. III. 2.](#)

⁶⁹ Vgl. [Teil 3 E. I. 3.](#)

⁷⁰ Vgl. [Teil 3 E. III. 1.](#)

⁷¹ „Kontrollratsgesetz“, *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 26.

wurde.⁷² Dabei können die Normen des BNDG grundsätzlich übernommen werden, wobei im Detail Änderungen notwendig sind.

a. Kontrollgegenstand des gerichtsähnlichen Kontrollorgans

Dies betrifft zunächst den Kontrollgegenstand für die Vorabkontrolle durch das gerichtsähnliche Kontrollorgan.

aa) Kontrolle der strategischen Ausland-Fermeldeüberwachung

Um sicherzustellen, dass das Kontrolldesign einer Prüfung durch den EGMR standhalten würde, sollte das GeKon künftig zumindest Kategorien von Selektoren genehmigen⁷³. Denkbar wäre zudem, dem GeKon einen vollumfänglichen Zugang zu den Suchbegriffen einzurichten, sodass es diese prüfen kann; was nicht heißt, dass es das in jedem Einzelfall auch tun muss.⁷⁴ Aus verfassungsrechtlichen Gründen müssten außerdem die Selektoren für gezielt personenbezogene Überwachungen in der Anordnung konkret benannt werden.⁷⁵ Die Ausnahme von der Genehmigungszuständigkeit zugunsten der G 10-Kommission (§ 23 Abs. 5 S. 2, 3 BNDG) ist wegen der Auflösung der G 10-Kommission gegenstandslos und müsste gestrichen werden.

bb) Vorabkontrolle von Vereinbarungen mit ausländischen Partnerdiensten

Bereits im Rahmen der Debatte über die Einführung des UKRats wurde zu Recht gefordert, dass dem GeKon „Absichtserklärungen“ für neue Vereinbarungen des BND mit ausländischen Partnerdiensten zur Genehmigung vorgelegt werden sollten. Auf diese Weise lässt sich die Anforderung des Bundesverfassungsgerichts absichern, wonach die Third Party Rule jedenfalls bei zukünftigen Vereinbarungen nicht mehr als Kontrollbarriere geltend gemacht werden kann. Für eine solche Vorlagepflicht spricht, dass die nachträgliche Kontrolle der Vereinbarungen aufgrund ihrer Bindungswirkung für den BND zu spät kommen kann.⁷⁶

Deshalb sollten die Nachrichtendienste nach dem vorgeschlagenen Kontrolldesign neue Absichtserklärungen vorab genehmigen lassen müssen.

⁷² Wetzling/Vieth, Mehr Rechtskontrolle wagen, S. 2, 18.

⁷³ Vgl. [Teil 3 C. II. 1. a. aa. \(2\)](#).

⁷⁴ Wetzling, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 9.

⁷⁵ Vgl. [Teil 3 C. II. 1. a. bb. \(2\)](#); Vogt, DöV 76 (2023), 689, 698.

⁷⁶ Markard, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 8.

cc) Ausweitung auf alle eingriffsintensiven nachrichtendienstlichen Befugnisse

Darüber hinaus müsste ein Kontrollratsgesetz eine Vorabkontrolle durch das GeKon mindestens etablieren für⁷⁷:

- strategische Beschränkungen gem. § 1 Abs. 1 Nr. 1 i. V. m. §§ 3 ff. G 10 und gem. § 5 G 10,
- längerfristige Observationen gem. § 8 Abs. 2 BVerfSchG, § 5 Abs. 2 BNDG i. V. m. § 8 Abs. 2 BVerfSchG, § 4 Abs. 1 MADG i. V. m. § 8 Abs. 2 BVerfSchG,
- den Einsatz von Vertrauensleuten und Verdeckten Ermittlern gem. §§ 9 a, b BVerfSchG, § 5 BNDG i. V. m. §§ 9 a, b BVerfSchG, § 5 Abs. 1 Hs.2 MADG i. V. m. §§ 9 a, b BVerfSchG,⁷⁸
- die Rechtsgrundlagen zur Identifizierung und Lokalisierung von mobilen Telekommunikations-Endgeräten unter Einsatz des sog. IMSI/IMEI-Catchers gem. § 9 Abs. 4 BVerfSchG, § 5 BNDG i. V. m. § 9 Abs. 4 BVerfSchG, § 5 MADG i. V. m. § 9 Abs. 4 BVerfSchG.
- die Entscheidung zur Aussetzung der Benachrichtigung von Betroffenen gem. § 15 Abs. 7 G 10.

Inwieweit die Tätigkeit des BND im Ausland, die über die normierten Beschränkungen hinausgeht, Gegenstand der Vorabkontrolle sein muss, kann nicht beantwortet werden. Es ist es zwingend, in einem ersten Schritt alle Tätigkeiten des Nachrichtendienstes gesetzlich abzubilden und spezifische Rechtsgrundlagen zu normieren⁷⁹. Erst dann kann entschieden werden, für welche Maßnahmen eine Genehmigung einzuholen ist. Das gilt unter anderem auch für das Militärische Nachrichtenwesen und HUMINT-Einsätze des BND⁸⁰.

Diese Aufzählung ist daher nicht abschließend.

⁷⁷ Vgl. [Teil 3 A. II.](#)

⁷⁸ Denkbar wären insoweit auch Abstufungen wie nach dem bayerischen Gesetzesentwurf, vgl. [Teil 4 B. II. 3. b. aa\) \(4\).](#)

⁷⁹ Vgl. [Teil 1 B. III. 4.](#)

⁸⁰ Insoweit muss der Hinweis von Dietrich beachtet werden, wonach wegen einer hohen Anzahl an HUMINT-Einsätzen eine „groß[e] Dynamik“ herrsche, die drohe, die Kontrollmechanismen zu stark zu hemmen, *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 25; eine Vorabkontrolle von Einsätzen des Militärischen Nachrichtenwesens fordert *Wetzling*, Bedingt kontrollfähig, S. 11.

dd) Vorabkontrolle in Eilfällen

Es ist positiv zu bewerten, dass der BND selbst in Eilfällen de lege lata eine Genehmigung durch das GeKon anfordern muss⁸¹. Dabei ist jedoch von entscheidender Bedeutung, dass die Maßnahmen durch die Vorabkontrolle nicht verunmöglicht werden. Deshalb hatte der Gesetzgeber für Eilfälle vorgesehen, dass zunächst eine Vorabgenehmigung durch ein einzelnes Mitglied des GeKon ausreichend ist und die Zustimmung der entsprechenden Kammer des GeKon zu der Maßnahme „unverzüglich“ nachgeholt werden muss. Offenbar gibt es trotzdem Fälle, in denen selbst eine Einbindung des „Eilfallrichters“ zu einer unvermeidbaren Verzögerung führen würde, weil sofortiges Handeln erforderlich ist.⁸² Für diese Fälle, bei denen es sich nach der Rechtsprechung des EGMR um Ausnahmen handeln muss⁸³, kann von einer Vorabgenehmigung abgesehen werden, sofern die Kontrolle sofort nachgeholt wird. Um abzusichern, dass diese Ausnahme von der Vorabkontrolle nicht zu weit gehandhabt wird, sollte jeder Fall dokumentiert und in bestimmten Abständen dem PKGr gemeldet werden. Der Gesetzgeber hat dann das Hintergrundwissen, um nachzusteuern, wenn er es für erforderlich hält. Durch eine solche Regelung besteht für die Nachrichtendienste zugleich ein Anreiz, von dieser Möglichkeit nicht allzu häufig Gebrauch zu machen.

b. Kontrolleur

Es wäre denkbar, die Mitglieder des GeKon um einen Betroffenenvertreter zu erweitern (aa)). Darüber hinaus sollte ein Mechanismus ergänzt werden, mit dem Konflikte innerhalb des GeKon unwahrscheinlicher werden (bb)). Zudem sollte das GeKon auch für Bewerber geöffnet werden, die nicht über langjährige Berufserfahrung als Richter am BGH oder BVerwG verfügen (cc)). Schließlich muss das PKGr bei der Wahl zukünftig eine echte Auswahlmöglichkeit haben (dd)).

aa) Betroffenenvertreter

Betroffene haben keine Möglichkeit, ihre Belange vor der Genehmigungsentscheidung und während der Durchführung der Maßnahme einzubringen, weil die Maßnahme und damit auch das Genehmigungsverfahren heimlich erfolgen. Diese Geheimhaltung ist unabdingbar, damit der Erfolg der Maßnahme nicht gefährdet wird.

⁸¹ Vgl. [Teil 3 C. II. 1. a.](#)

⁸² *Hoch/Schmidt-Räntsch/Brunst*, NVwZ 2023, 712, 715.

⁸³ Vgl. [Teil 2 B. I. 4. a. aa\).](#)

(1) Vor- und Nachteile

Um dennoch sicherzustellen, dass die Betroffenenperspektive in den Überlegungen der Kontrolleure Berücksichtigung findet, wird vorgeschlagen, das Genehmigungsverfahren kontradiktorisch auszugestalten: Dafür soll an Stelle des Betroffenen eine Person eingebunden werden, die dessen Interessen vertritt.⁸⁴ Ähnliche Regelungen existieren für den Bereich der Auslandsaufklärung bereits in Schweden und den USA.⁸⁵ Für eine derartige Regelung spricht, dass auch der EGMR – jedenfalls bezogen auf die nachträgliche Kontrolle – bereits Sympathie für die Einbindung eines Betroffenenvertreters bekundet hat.⁸⁶

Wetzling fordert darüber hinaus unter anderem die Einbeziehung einer Person, die „das Vertrauen der Vertreter:innen von besonders schützenswerter Kommunikation (z.B. Anwält:innen, Journalist:innen, Gläubige) genießt“.⁸⁷ Möglicherweise könnte ein Betroffenenvertreter auch diese Funktion wahrnehmen.

Gegen die Notwendigkeit der Etablierung eines Betroffenenvertreters spricht die verfassungsrechtliche Herleitung der unabhängigen Rechtskontrolle: Der Kontrolleur soll die Rechtmäßigkeit einer gegen einen Betroffenen gerichteten Maßnahme prüfen, weil der Betroffene selbst es wegen der Heimlichkeit nicht kann. Die Betroffenenperspektive zu berücksichtigen, ist damit Kernaufgabe des Kontrolleurs selbst.⁸⁸

⁸⁴ *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 14 f.; *Deutscher Anwaltverein*, Stellungnahme zum Regierungsentwurf eines Gesetzes zur Änderung des BNDG, S. 38; Dt. Bundestag, Antrag der Fraktion Bündnis 90/die Grünen, Drs. 19/26221 v. 27.1.2021, S. 8; bzgl. der G 10-Kommission Dt. Bundestag, Antrag der FDP-Fraktion, Drs. 19/19509 v. 26.5.2020, S. 3; „Eine derartige Effektivierung der Kontrolle durch die Möglichkeit, die Betroffenen ihre Rechte jedenfalls treuhänderisch geltend zu machen, ließe sich nach hiesiger Ansicht unmittelbar aus den Verhältnismäßigkeitsanforderungen im engeren Sinne an einen besonders schweren heimlichen Eingriff in Art. 10 Abs. 1 GG. ableiten.“, *Vogt*, Strategische Auslandstelekommunikationsüberwachung 2023, S. 658; Bürgerrechtsanwalt zur G 10-Kommission bei *Bantlin*, G 10-Kommission, S. 231 ff.; Dreier/Brosius-Gersdorf/*Wischmeyer*, Art. 10 GG Rn. 98.

⁸⁵ *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 13 f., der einen ehemaligen Bundesrichter am amerikanischen Foreign Intelligence Surveillance Court, James Robertson, zitiert: „To avoid being a rubber stamp, the process needed an adversary (...) to challenge and take the other side of anything that is presented to the FISA Court. Judges are learned in the law and all that, but anybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding“, <https://slate.com/technology/2020/05/usa-freedom-reauthorization-act-fisa-reform-surveillance-amicus-curiae.html>, (abgerufen am 31.8.2024); dazu auch *Donohue*, The Future of Foreign Intelligence, S. 144 f.; *Bantlin*, G 10-Kommission, S. 225 ff.

⁸⁶ Wenn möglich, solle das Verfahren kontradiktorisch organisiert sein, vgl. [Teil 2 B. I. 4. b. ff.](#); *Vogt*, Strategische Auslandstelekommunikationsüberwachung, S. 658.

⁸⁷ *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 13 f.

⁸⁸ Vgl. die verfassungsrechtliche Bewertung [Teil 2 A. IV. 2. a. bb.](#); *Hoch/Schmidt-Räntsch/Brunst*, NVwZ 2023, 712, 715, das fehlende rechtliche Gehör sei „(...) kein Mangel, sondern geradezu der Sinn des Verfahrens“, der Richtervorbehalt sei „eine Art externalisierter Selbstkontrolle der Verwaltung“.

So gesehen ist die Einführung eines Betroffenenvertreters nicht zwingend notwendig. Andererseits ändert sich an der Rolle des UKRats nichts, wenn es einen dezidierten Betroffenenvertreter gibt. Je nachdem, wie die Beratungen in der Praxis ablaufen, kann dessen Einbindung die Interessen des Betroffenen tatsächlich stärken. Jedenfalls würde der Gesetzgeber mit dessen Einführung rechtspolitisch verdeutlichen, dass ihm die Betroffenenperspektive wichtig ist. Das kann für sich genommen Grund genug sein, sich für die Etablierung eines Betroffenenvertreters zu entscheiden.

(2) Ausgestaltung

Denkbar wäre, jeder Kammer des GeKons einen Betroffenenvertreter zuzuordnen. Bei der Ausgestaltung ist darauf zu achten, dass dessen Beteiligung nicht dazu führen darf, dass das Genehmigungsverfahren insgesamt zu lange dauert und die Effektivität der Maßnahme dadurch gefährdet wird.⁸⁹

Um die Neutralität des Verfahrens zu wahren und einen Konflikt mit der Third Party Rule zu verhindern, aber dennoch die Betroffenenperspektive zu stärken, wird von Mitgliedern des UKRat empfohlen, anstatt einer externen Person einen Richter des UKRat damit zu beauftragen, in dem jeweiligen Verfahren die Betroffenenperspektive einzunehmen.⁹⁰ Dagegen spricht, dass dieser Betroffenenanwalt zugleich Mitglied des entscheidenden, gerichtsähnlichen Kontrollorgans ist und daher eigentlich eine andere Funktion wahrnimmt, in der er neutral entscheiden soll. Wie auf diese Weise die Betroffenenperspektive gestärkt werden soll, ist unklar. Da das GeKon bei der Entscheidungsfindung ohnehin die Betroffenenperspektive berücksichtigen muss, bietet diese Lösung zudem keinen Vorteil zur aktuellen Ausgestaltung.

Bantlin schlägt vor, dass die G 10-Kommission diese Rolle im Rahmen eines Gerichtsverfahrens übernimmt.⁹¹ Diesen Gedanken aufnehmend wäre es denkbar, die Mitglieder der nach diesem Vorschlag aufgelösten G 10-Kommission als Betroffenenvertreter einzusetzen, die die Betroffeneninteressen vor dem UKRat und nicht vor Gericht vertreten.

Insgesamt ist zu bedenken, dass die Einbindung eines Betroffenenvertreters nicht automatisch zu einer besseren Berücksichtigung der Betroffenenperspektive führen muss. Wichtig ist, organisatorisch sicherzustellen, dass der Betroffenenvertreter trotz der generellen Eilbedürftigkeit von nachrichtendienstlichen Anordnungen und seinem Unvermögen, den Betroffenen zu kontaktieren, in überzeugender Weise für die Rechte des Betroffenen eintreten kann:

⁸⁹ *Hoch/Schmidt-Räntsch/Brunst*, NVwZ 2023, 712, 715.

⁹⁰ *Hoch/Schmidt-Räntsch/Brunst*, NVwZ 2023, 712, 715.

⁹¹ Das Gerichtsverfahren wird auch von der G 10-Kommission initiiert, *Bantlin*, G 10-Kommission, S. 234 ff.

„The risk is that the advocate becomes a hostage of the proceedings, and serves simply as a legitimisation of a – foregone – conclusion.“⁹²

Nur wenn das verhindert wird, wäre mit der Einführung eines Betroffenenvertreters wirklich etwas gewonnen.

bb) Eingabemöglichkeit an das PKGr

In diesem Kontrolldesign sollten sich einzelne Mitglieder des GeKon in absoluten Ausnahmefällen anonym an das PKGr wenden können.

(1) Grund

Es darf nicht unterschätzt werden, dass zwischen den Mitgliedern des GeKon ein hohes Konfliktpotenzial besteht, weil die rechtlichen Grundlagen weit gefasst sind und somit einen großen Entscheidungs- und Interpretationsspielraum lassen⁹³. Dadurch können mitunter fundamentale, vermeintlich unüberbrückbare Meinungsverschiedenheiten entstehen, die im schlimmsten Fall die Arbeitsfähigkeit des GeKon massiv beeinträchtigt können. Hinter dem Vorschlag für eine Whistleblower-Schutznorm an das PKGr steht die Überlegung, dass schon die Möglichkeit, Dritte zu informieren, rationalisierend wirkt und somit die Wahrscheinlichkeit von unüberwindbaren Problemen innerhalb des GeKons erheblich senkt. Das PKGr bietet sich als Adressat der Eingabe an, weil es sich mit der Kontrolltätigkeit des GeKon ohnehin auseinandersetzt, denn unter anderem muss das GeKon ihm regelmäßig Bericht erstatten (§ 55 Abs. 1 BNDG)⁹⁴.

(2) Mögliche Einwände

Gegen eine solche Norm lässt sich anführen, dass das PKGr nicht die (rechtlichen) Möglichkeiten hat, um einen Konflikt zu beenden oder zugunsten einer Partei einzugreifen. Eine solche übergeordnete Rolle darf es schon wegen der verfassungsrechtlich zwingenden Unabhängigkeit des GeKon nicht wahrnehmen. Das wirft die Frage auf, was überhaupt der Vorteil einer solchen Eingabe wäre. Ein Vorteil besteht darin, dass schon die rechtliche Möglichkeit, tiefgehende Konflikte nach „außen“ tragen zu können, die Kompromissbereitschaft innerhalb des Gremiums erhöhen wird. Hinzu kommt, dass die Offenlegung schwerwiegender Probleme gegenüber den Mitgliedern

⁹² Venedig-Kommission, Report 2015, S. 49 Rn. 225.

⁹³ Vgl. [Teil 2 A. IV. 2. c.](#)

⁹⁴ Vgl. [Teil 3 C. IX. 3.](#)

des PKGr mit einem Ansehensverlust der Mitglieder des GeKon einhergehen kann. Es ist davon auszugehen, dass ein solcher Ansehensverlust nicht im Interesse der renommierten Persönlichkeiten liegt, die dem GeKon angehören und deshalb rationalisierend auf die Diskussionskultur im GeKon wirken kann.

Als weiteren Einwand gegen eine Meldemöglichkeit lässt sich anführen, dass die Beratungen des GeKon geheim sind (§ 54 Abs. 1, 2 BNDG). Über die Erteilung einer Aussagegenehmigung entscheidet der Präsident des UKRat (§ 54 Abs. 3 BNDG). Außerdem enthält § 3 S. 1 der Geschäftsordnung des UKRat⁹⁵ eine mit dem richterlichen Beratungsgeheimnis gem. § 43 DRiG vergleichbare Norm. Demnach haben „(...) die zur Entscheidung berufenen Mitglieder des gerichtsähnlichen Kontrollorgans über den Hergang bei der Beratung und Abstimmung in den Spruchkörpern auch nach Beendigung ihres Dienstverhältnisses zu schweigen“.

Die hier vorgeschlagene Berichtsmöglichkeit an das PKGr widerspricht sowohl der Geheimhaltungspflicht und dem Entscheidungsvorbehalt des UKRats-Präsidenten gem. § 54 BNDG als auch § 3 S. 1 GO UKRat. Der Gesetzgeber kann eine davon abweichende Regelung treffen, die der Geschäftsordnung wegen Höherrangigkeit vorgehen würde, wenn andere Vorschriften dem nicht entgegenstehen. § 43 Deutsches Richtergesetz (DRiG), der das richterliche Beratungsgeheimnis regelt, ist neben § 54 Abs. 1, 2 BNDG nicht anwendbar, da der Gesetzgeber – anders als in anderen Normen zum UKRat⁹⁶ – nicht darauf verweist. Deshalb ist § 43 DRiG kein Hindernis. Allerdings ist das richterliche Beratungsgeheimnis gem. Art. 97 Abs. 1 GG als Bestandteil der richterlichen Unabhängigkeit im höherrangigen Recht verankert.⁹⁷ Art. 97 GG ist auf die richterähnliche Kontrolle durch den GeKon allerdings nicht direkt anwendbar, weil dessen Mitglieder keine Richter i. S. d. Art. 97 GG sind.

Dass Art. 97 GG in all seinen Ausprägungen analog zu beachten ist, lässt sich allenfalls aus der Vorgabe des Bundesverfassungsgerichts folgern, wonach die unabhängige Vorabkontrolle richterlich oder „richterähnlich“ auszugestalten sei. Selbst dann wäre der Eingriff in die Unabhängigkeit gerechtfertigt, weil diese Ausnahme von der Geheimhaltung nach der hier vertretenen Auffassung erforderlich ist, um die Funktionsfähigkeit des Gremiums abzusichern.

⁹⁵ Unabhängiger Kontrollrat, Bekanntmachung der Geschäftsordnung v. 12.12.2021, BAnz AT 27.12.2021 B4, <https://www.bundesanzeiger.de/pub/de/amtliche-veroeffentlichung?5> (abgerufen am 31.8.2024).

⁹⁶ §§ 45 Abs. 4, 47 Abs. 2 BNDG.

⁹⁷ *Fahrner*, GSZ 2023, 223, 226; *Einsiedler*, NJ 2014, 6, 7.

(3) Enge Ausgestaltung

Neben dem GeKon als Organ, das ohnehin berechtigt ist, sich an das PKGr zu wenden, sollte diese Möglichkeit auch Mitgliedern offenstehen, um so die Minderheitenrechte der einzelnen Mitglieder des Gremiums zu stärken⁹⁸.

Um die Unabhängigkeit des GeKon von der Legislative sicherzustellen, muss eine solche Eingabemöglichkeit auf Ausnahmekonstellationen begrenzt sein. Das bedeutet, dass das PKGr über einmalige Meinungsverschiedenheiten oder Konflikte nicht benachrichtigt werden darf. Stattdessen muss das eingebende Mitglied überzeugt sein, dass die Arbeitsfähigkeit des Gremiums durch eine über den Einzelfall hinausgehende Streitigkeit stark beeinträchtigt ist.

Eine solche Norm kann dazu beitragen, einer wegen unüberbrückbarer Differenzen entstehenden Lähmung des unabhängigen GeKon vorzubeugen.

cc) Öffnung des Bewerberkreises

Gem. § 43 Abs. 1 BNDG muss das GeKon mit Personen besetzt werden, die bis zu ihrer Ernennung Richterinnen am BGH oder am BVerwG waren und über eine langjährige Berufserfahrung verfügen. Dieser enge (und ursprünglich sogar noch enger geplante Bewerberpool) wurde vor der Verabschiedung der letzten BNDG-Reform zu Recht scharf kritisiert⁹⁹. Warum nur Personen aus diesem Kreis geeignet sein sollen, ist nicht ersichtlich. Es ist im Gegenteil sogar davon auszugehen, dass diversere Perspektiven die Diskussion bereichern. Daher sollten zumindest auch andere Richter sich beim PKGr bewerben können.¹⁰⁰ Besonders die Verwaltungsrichter am Sitz des BfV und der Landesverfassungsschutzbehörden, die für Klagen gegen die Nachrichtendienste zuständig sind, erscheinen hierfür wegen ihrer Berufserfahrungen prädestiniert.

Das Bundesverfassungsgericht hat festgelegt, dass der „richterlichen Perspektive ein maßgebliches Gewicht“ beizumessen ist, weshalb eine „maßgebliche Zahl“ der Stellen mit langjährig erfahrenen Richtern zu besetzen sei.¹⁰¹ Wann eine „maßgebliche Zahl“ erreicht ist, kann gesetzgeberisch konkretisiert werden. Sie dürfte vermutlich erst er-

⁹⁸ Vgl. [Teil 2 A. IV. 2. d. aa.](#)

⁹⁹ Vgl. [Teil 3 C. IV. 1. b.](#)

¹⁰⁰ Für die mit der nach der Amtszeit folgende Rückkehr in die Landesjustiz und der Konsequenzen einer unterschiedlichen Besoldung für das Ruhegehalt wird sich sicherlich eine Lösung auftun; u.a. auch in Bezug auf Richter an Oberlandesgerichten, *Löffelmann*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BNDG, S. 21 sowie zusätzlich Richter an Obergerichtungen *Graulich*, GSZ 2021, 121, 128; *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 22.

¹⁰¹ Vgl. [Teil 2 A. III. 1. a. ii\).](#)

reicht sein, wenn mindestens die Hälfte mit erfahrenen Richtern besetzt ist. Andererseits kann mit der Formulierung definitiv nicht gemeint sein, dass alle Stellen durch langjährig erfahrene Richter zu besetzen sind.

Es ist verfassungsrechtlich also durchaus möglich, neben den Richtern Volljuristen oder andere Berufsgruppen, wie beispielsweise Politikwissenschaftler mit Expertise im Nachrichtendienstrecht, einzubinden.¹⁰²

Alternativ regen zwei der aktuellen Mitglieder des GeKon und der Leiter des AdKon an, dem Generalbundesanwalt ein Vorschlagsrecht zu verleihen, sodass zukünftig auch Bundesanwältinnen und Bundesanwälte Mitglieder des GeKon sein könnten. Bundesanwälte seien erstens mit nachrichtendienstlichen Phänomenen betraut und zweitens „in der Lage, die Interessen der Betroffenen angemessen zu berücksichtigen“, weil sie als Staatsanwälte darin geschult seien, die unterschiedlichen Umstände aufzuklären.¹⁰³

Fabrner hingegen warnt vor der Ernennung von Bundesanwälten, denn es sei mit Blick auf die gebotene Unabhängigkeit nicht empfehlenswert, Personengruppen „mit zuvor zu sehr prägender ‚Sozialisierung‘ im Bereich der Exekutive“ zu wählen.¹⁰⁴ Wie bereits bei den Richtern, gibt es bei den Staatsanwälten keinen zwingenden Grund, die Tätigkeit an einem obersten Bundesgericht zur Bewerbungsvoraussetzung zu machen. Denn Staatsanwälte unterer Stufen sind ebenso darin geschult, unterschiedliche Umstände aufzuklären.¹⁰⁵ So wie Richtern, die in ihrem Berufsalltag zuvor keine Berührungspunkte zum Nachrichtendienst hatten, dürfte es auch Staatsanwälten möglich sein, sich einzuarbeiten.

Eine Öffnung des Bewerberkreises auf Berufsgruppen mit weniger attraktivem Gehalt als dem eines obersten Bundesrichters hätte den Vorteil, dass es unproblematischer wäre, die Besoldung abzusenken. Mit der hohen Besoldung soll den Obersten Bundesrichtern ein lukrativer Anreiz für einen Wechsel zum GeKon geboten werden.¹⁰⁶ Das führt dazu, dass der Präsident des UKRats so viel verdient wie die Präsidenten von BND und BfV, Mitglieder des GeKon immerhin so viel wie die Präsidentin des MAD, vgl. § 46 BNDG. Sollte die Zuständigkeit des GeKon auf die Vorabkontrolle aller eingriffsintensiven nachrichtendienstlichen Mittel ausgeweitet werden, muss das GeKon deutlich vergrößert werden. Je nachdem, wie viele neue Stellen notwendig sind, werden

¹⁰² Da vier der fünf Mitglieder der aktuellen G 10-Kommission Volljuristen sind (während nur einer von ihnen als Richter gearbeitet hat), könnten so unter anderem alle Mitglieder der G 10-Kommission in das GeKon aufgenommen werden.

¹⁰³ *Hoch/Schmidt-Räntsch/Brunst*, NVwZ 2023, 712, 713.

¹⁰⁴ *Fabrner*, GSZ 2023, 223, 225; ähnlich bereits Schwabenbauer zur G 10-Kommission, der davor warnt, Mitglieder zu ernennen, bei denen es sich um „ausgeschiedene Angehörige“ der Nachrichtendienste handelt, *Schwabenbauer*, Heimliche Grundrechtseingriffe, S. 350.

¹⁰⁵ Graulich schlägt ebenfalls die Einbindung von Staatsanwälten unterschiedlicher Stufen vor, *Graulich*, GSZ 2021, 121, 128.

¹⁰⁶ *Graulich*, GSZ 2021, 121, 128.

sich die Personalausgaben vervielfachen. Angesichts der bereits jetzt häufig geäußerten Kritik, dass in Deutschland die Kontrolle wichtiger sei als die eigentliche nachrichtendienstliche Arbeit¹⁰⁷, sollte erwogen werden, die Besoldung für die künftigen Mitglieder abzusenken.

dd) Auswahlmöglichkeit des Parlamentarischen Kontrollgremiums

Weil die Präsidenten der Obersten Bundesgerichte gerade so viele Kandidaten vorschlagen haben, wie es Sitze zu besetzen gab, hatte das PKGr bei der ersten Besetzung des GeKons Berichten zu Folge de facto kein Wahlrecht, was dazu führte, dass die Mitglieder von den Präsidenten der Obersten Bundesgerichte „ernannt“ wurden.

Zukünftig sollte das PKGr aus einem entsprechenden Pool von Bewerbern auswählen können. Um das sicherzustellen, sollten Interessierte die Möglichkeit haben, ihre Bewerbung direkt an das PKGr zu richten.

c. Distanz

Das GeKon sollte das Bundeskanzleramt vor seinem Bericht an das PKGr nicht anhören müssen. Deshalb sollte § 55 Abs. 2, 3 BNDG gestrichen werden¹⁰⁸.

Darüber hinaus sollte § 41 Abs. 6 BNDG klarstellend um den Satz ergänzt werden, dass das GeKon nicht beim BND angesiedelt werden darf, um eine räumliche Distanz zwischen Kontrolleur und Kontrolliertem sicherzustellen.¹⁰⁹

d. Initiative

Das GeKon genehmigt die Anträge, die der BND ihm zur Vorabkontrolle vorlegt. Die Initiative liegt somit beim Kontrollierten¹¹⁰.

aa) Beschwerderecht der Betroffenen

Das Bundesverfassungsgericht hat den Gesetzgeber beauftragt, zu prüfen, ob potenziell von strategischen Ausland-Fernmeldeüberwachungen Betroffene das Recht haben sollten, die gerichtsähnliche Kontrolle anzustoßen und in diesem Prozess mit Verfahrensrechten ausgestattet zu sein.¹¹¹ Eine solche Beschwerdemöglichkeit hat der Gesetzgeber

¹⁰⁷ „Diese ausufernde Kontrollbürokratie ist die Schwester der Ineffizienz“, *Hanning/Schindler*, Gastbeitrag.

¹⁰⁸ Vgl. [Teil 3 C. V.](#)

¹⁰⁹ Vgl. [Teil 3 C. V.](#)

¹¹⁰ Vgl. [Teil 3 C. VII.](#)

¹¹¹ Vgl. [Teil 2 A. III. 1. b. ff.](#), BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 280.

nicht eingeführt. Im Gegensatz zum UKRat wird die G 10-Kommission gem. § 15 Abs. 5 S. 1 G 10 auf Antrag von Betroffenen tätig.¹¹² Dasselbe gilt gem. § 28 Abs. 1 BVerfSchG für den BfDI.

Wieso ein Beschwerderecht gegenüber der G10-Kommission und dem BfDI existiert, gegenüber dem UKRat jedoch nicht, ist nicht nachvollziehbar.¹¹³

Zudem spricht das Konventionsrecht dafür, ein Beschwerderecht zu etablieren. Nach der Rechtsprechung des EGMR müssen Betroffene die Möglichkeit haben, die Rechtmäßigkeit von Überwachungsmaßnahmen ex-post zu kontrollieren. Dafür gibt es grundsätzlich zwei Optionen: Entweder der Betroffene wird anschließend benachrichtigt und somit in die Lage versetzt, einen gerichtlichen Rechtsbehelf zu verfolgen; oder es gibt eine gesetzliche Möglichkeit, sich gegen die Maßnahme wehren zu können, ohne eine konkrete Betroffenheit nachweisen zu müssen. Der EGMR macht deutlich, dass er die zweite Option präferiert. Im Bereich der strategischen Überwachung ist dies Teil der zur Konventionskonformität zwingend einzuhaltenden „Ende zu Ende-Schutzmechanismen“.¹¹⁴

Steiner hat daher zu Recht festgestellt, dass ein ex post-Rechtsbehelf für potenziell Betroffene nach der Rechtsprechung des EGMR von zentraler Bedeutung ist. Der grundsätzlich offenstehende Rechtsweg zum Bundesverwaltungsgericht kann diese Funktion im Nachrichtendienstrecht allerdings nicht erfüllen, weil es den Betroffenen mangels Benachrichtigung über eine Beobachtung überwiegend unmöglich sein wird, ihre Betroffenheit so darzulegen, dass die Hürde der Klagebefugnis überwunden wird.¹¹⁵

Insbesondere für Ausländer im Ausland ist der klassische Rechtsweg wegen der „kaum überwindbaren Anforderungen an die Konkretisierung des Streitgegenstands (...) praktisch nicht verfügbar“.¹¹⁶

Um das Kontrolldesign dennoch konventionskonform auszugestalten, muss Betroffenen deshalb die Möglichkeit verliehen werden, sich unabhängig vom Nachweis einer tatsächlichen Betroffenheit nachträglich gegen strategische Überwachung wehren zu können.¹¹⁷ Auch bei gezielten Maßnahmen betont der EGMR, dass wirksame ex-post Kontrollen notwendig sind und dass er eine Regelung präferiert, bei der Betroffene die Kontrolle unabhängig von einem Nachweis konkreter Betroffenheit anstoßen können.¹¹⁸

¹¹² *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 24.

¹¹³ So auch *Vogt*, DöV 76 (2023), 689, 698.

¹¹⁴ Vgl. [Teil 2 B. I. 4. b. ff.](#)

¹¹⁵ *Steiner*, GSZ 2024, 32, 37.

¹¹⁶ *Bäcker*, Beschwerdeschrift BNDG II, S. 103 f.

¹¹⁷ Steiner bezeichnet das Fehlen einer solchen Beschwerdemöglichkeit als „wesentliche konventionsrechtliche Schwäche des deutschen Rechts“, *Steiner*, GSZ 2024, 32, 37.

¹¹⁸ Vgl. [Teil 2 B. I. 4. a. cc.](#)

Um zu verhindern, dass Betroffene „nicht zu bloßen Objekten der Überwachung“¹¹⁹ werden, sollte daher ein Beschwerderecht für alle Maßnahmen, für deren Genehmigung das GeKon zuständig ist, eingeführt werden.¹²⁰ Das GeKon kommt als Kontrolleur auf der dritten Stufe nach der Rechtsprechung des EGMR jedoch nur in Betracht, wenn zwei Aspekte gesetzlich angepasst werden.

Erstens muss auf jeder der drei Kontrollstufen ein anderer Kontrolleur vorgesehen sein, um Interessenkonflikte zu verhindern. Da das GeKon auch auf der ersten Stufe für die Genehmigung der Maßnahmen zuständig ist, wäre ein Beschwerderecht an das GeKon grundsätzlich nicht konventionskonform. Der EGMR hat hiervon jedoch eine Ausnahme für den Fall zugelassen, dass der Kontrolleur selbst effektiv kontrolliert wird. Die Kontrollen des Kontrolleurs müssten aber regelmäßig erfolgen, was auch gesetzlich geregelt sein muss.¹²¹

Als Kontrolleur des Kontrolleurs kommt nach deutschem Recht der BfDI in Betracht, der bereits für die Kontrolle des UKRats zuständig ist. Dazu bedarf es jedoch noch einer gesetzlichen Klarstellung im Kontrollratsgesetz dahingehend, dass die Kontrollen des BfDI regelmäßig erfolgen und sich auch auf den Umgang mit Betroffenenbeschwerden erstrecken.

Zweitens müssen die begründeten Entscheidungen des GeKon über Betroffenenbeschwerden gegenüber den Betroffenen, mindestens aber gegenüber sicherheitsüberprüften Anwälten offengelegt werden.¹²² Eine solche Begründungspflicht für Entscheidungen des GeKon müsste in das Kontrollratsgesetz aufgenommen werden.¹²³ Die Einsichtnahme der Begründung auf sicherheitsüberprüfte Anwälte zu begrenzen, hätte den Vorteil, dass „Testbeschwerden“ ausgeschlossen werden, mit denen Dritte versuchen könnten, herauszufinden, ob sie nachrichtendienstlich beobachtet werden.¹²⁴

Nur wenn diese zwei Aspekte berücksichtigt werden, ist davon auszugehen, dass ein ex post-Rechtsbehelf zum GeKon einer Prüfung durch den EGMR standhalten würde.

¹¹⁹ Bäcker, Beschwerdeschrift BNDG II, S. 103.

¹²⁰ Dem stehen auch drei der aktuellen Mitglieder des GeKon offen gegenüber: *Hoch/Schmidt-Räntsch/Brunst*, NVwZ 2023, 712, 715; *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 24; *Vogt*, DöV 2023, 689, 698.

¹²¹ Vgl. [Teil 2 B. I. 4. b. ff.](#)

¹²² Vgl. [Teil 2 B. I. 4. b. ff.](#)

¹²³ Vgl. [Teil 4 B. 3. f. aa\). \(1\).](#)

¹²⁴ Zur G 10-Kommission *Arndt*, G 10-Verfahren, 43, 57; *Schenke/Graulich/Ruthig/Huber*, § 15 G 10 Rn. 39.

bb) Direkter digitaler Zugriff

Zwingende Voraussetzung wirksamer Kontrollen ist, dass die Nachrichtendienste alle genehmigungspflichtigen Anordnungen und sonstigen notwendigen Informationen tatsächlich vorlegen. Obwohl die Einhaltung der Vorlagepflicht durch die interne Dienst- und Fachaufsicht und die externe Datenschutzkontrolle abgesichert wird, ist dennoch kritisch anzumerken, dass die Nachrichtendienste weiterhin entscheiden, was zu kontrollieren ist.¹²⁵ Um diese Abhängigkeit von den Nachrichtendiensten zu verringern, wird daher vorgeschlagen, dem Kontrolleur einen „direkten digitalen Zugriff auf die von den Nachrichtendiensten erhobenen Kommunikationsdaten sowie deren Überwachungsprogramme“ einzurichten und einen Export der Daten zu ermöglichen, damit die Kontrolleure sie analysieren können.¹²⁶ Ein solcher direkter digitaler Zugriff kommt nur für die (allerdings sehr umfangreiche) datenbasierte Nachrichtendienstarbeit in Betracht.

e. Kontrollmittel zur Informationsgewinnung

Die Kontrollmittel zur Informationsgewinnung sind bereits de lege lata weitgehend. Trotzdem wäre eine gesetzliche Nachschärfung mancher Aspekte zweckdienlich, um dem Kontrollierenden einen umfassenderen Eindruck des Ist-Zustands zu ermöglichen.

aa) Umfassende Protokollierung der Verarbeitungsschritte

Die Wirksamkeit der Kontrollmittel zur Informationsgewinnung ist davon abhängig, dass die Verarbeitungsschritte lückenlos protokolliert werden. Deshalb müssen die Nachrichtendienste zukünftig gesetzlich zur umfassenden Protokollierung ihrer Datenverarbeitungen verpflichtet werden.

bb) Beschwerdemöglichkeit für Whistleblower aus den Nachrichtendiensten

Darüber hinaus sollte eine Whistleblower-Schutznorm eingeführt werden, denn Eingaben von Whistleblowern ermöglichen dem Kontrolleur einen im Vergleich (nahezu)

¹²⁵ "Die Selbstverständlichkeit, dass der Gegenstand der Kontrolle vom Kontrolleur und nicht vom zu Kontrollierenden bestimmt wird", sei "bislang wenig ausgeprägt", zitiert Ronen Steinke den ehemaligen BND-Präsidenten Schindler in einem Interview vom 22.9.2016, *Steinke*, Früherer BND-Chef kritisiert Kontrollsystem des deutschen Geheimdiensts; *Wetzling*, Gastkommentar.

¹²⁶ *Wetzling/Vieth*, Datenbasierte Nachrichtendienstkontrolle, S. 56; *Wetzling*, Gastkommentar; *Wetzling/Vieth*, Gute Rechtsnormen und innovative Kontrollpraxis, S. 56.

ungefilterten Eindruck des Ist-Zustandes¹²⁷. Sie vertiefen so die Kenntnis des Kontrollleure über die Tatsachengrundlage des Vergleichs¹²⁸. Für die praktische Umsetzbarkeit dieser Idee spricht, dass im Nachrichtendienstrecht bereits an anderer Stelle vergleichbare Schutznormen etabliert sind: So können sich Whistleblower aus den Nachrichtendiensten auf der Bundesebene und in sieben Bundesländern bereits heute an das PKGr wenden.¹²⁹ Der Gesetzgeber könnte sich bei der Umsetzung an § 8 Abs. 1 PKGrG orientieren, der im Landesvergleich einen weitgehenden Schutz des Whistleblowers garantiert, da erstens der Dienstweg nicht vorab beschritten werden muss, zweitens ein Maßregelungs- und Benachteiligungsverbot vorgesehen ist und drittens der Name des Mitarbeiters nicht genannt werden darf. Diese Schutzvorkehrungen für den mitteilenden Whistleblower erhöhen die Wahrscheinlichkeit, dass von der Beschwerdemöglichkeit in der Praxis tatsächlich Gebrauch gemacht wird. Whistleblower sollten sich sowohl an den UKRat als auch an den BfDI wenden können.

cc) Anordnung

Was die Anordnungen der Nachrichtendienste angeht, die dem GeKon zur Genehmigung vorgelegt werden, sollte sichergestellt sein, dass sie ausreichend begründet sind (1.), was das GeKon im Zweifel erzwingen können muss (2.).

(1) Begründungstiefe

Aus der Rechtsprechung des Bundesverfassungsgerichts ergibt sich, dass die Nachrichtendienste den Vorabkontrolleur umfassend und substantiiert über alle relevanten Aspekte informieren müssen.¹³⁰ Die Norm zu den Voraussetzungen der Anordnungen, § 23 BNDG, sollte um die Klarstellung ergänzt werden, dass die Anordnungen umfassend begründet werden müssen.¹³¹

¹²⁷ Bantlin, G 10-Kommission, S. 94 ff.; Gusy, VerwArch 2015, 437, 443.

¹²⁸ Vgl. [Teil 1 A. III. 5](#). Für die praktische Relevanz dieser Normen kommt es jedoch entscheidend darauf an, dass die Whistleblower vor strafrechtlichen Sanktionen und bestenfalls auch vor Bekanntmachung ihrer Identität geschützt werden, vgl. dazu Bantlin, G 10-Kommission, S. 95, 96.

¹²⁹ Dabei wurde auf insgesamt drei Regelungsmodelle zurückgegriffen, Michel, GSZ 2021, 197, 203.

¹³⁰ Vgl. [Teil 2 A. III. 1. a. gg](#)), [Teil 2 A. III. 1. b. gg](#)); Bantlin/Graulich, GSZ 2023, 179, 182; in der Praxis ist dies nicht immer der Fall, was bereits die Mitglieder des Unabhängigen Gremiums kritisiert haben, Leyendecker/Pinkert, BND behindert Kontrollgremium.

¹³¹ Auch Wetzling schreibt: „Möglichst genaue Angaben im Antragstext sind wichtig, damit die gerichtähnliche Kontrolle prüfen kann, ob ein ausreichend begründetes Aufklärungsinteresse vorliegt.“, Wetzling, Bedingt kontrollfähig, S. 12.

Den Forderungen, wonach der Antragssteller die Verhältnismäßigkeit detailliert begründen sollte und in diesem Zusammenhang alternative, mildere Mittel nennen sollte, ist vollumfänglich zuzustimmen.¹³²

(2) Sanktionsbefugnis gegenüber dem BND

Wetzling weist darauf hin, dass Mitglieder europäischer Aufsichtsbehörden berichtet haben, „dass Anordnungen oftmals nur aus einer bestimmten Anzahl von Textbausteinen bestehen“ und „Argumente in Begründungstexten einfach (...) kopiert und eingefügt“ wurden und „eher phrasenhaft ohne inhaltlichen Gehalt“ formuliert worden sind. Damit das GeKon sich gegen solch oberflächlich begründete Anordnungen oder eine fehlende Mitwirkung der deutschen Nachrichtendienste wehren kann, fordert er „eine direkte Sanktionsbefugnis“ des BND.¹³³

Denkbar wäre, das Beanstandungsrecht gem. § 52 BNDG – in einer um zwei Anhörungsschleifen gekürzten Variante¹³⁴ – auf diese Situation auszuweiten. Effektiver wäre hingegen, dem GeKon eine generelle, verbindliche Anordnungsbefugnis zu verleihen, denn nur dann kann es eine ausreichend detaillierte Begründung erzwingen.

dd) Kontrollmittel für einzelne Mitglieder des GeKon

Da der unabhängige Vorabkontrolleur über beträchtliche Macht verfügt und wegen seiner Unabhängigkeit nicht kontrolliert wird, müssen den einzelnen Mitgliedern des GeKon Minderheitenrechte verliehen werden.¹³⁵ Anstatt für die Geltendmachung von Kontrollmitteln einen Mehrheitsbeschluss zu fordern, sollte jedes Mitglied daher zukünftig „eigenständige ergänzende Aufklärungs- und Informationsbeschaffungsrechte“ geltend machen können.¹³⁶

ee) Durchsetzungsinstrumente

Darüber hinaus muss sichergestellt sein, dass die Kontrollmittel des GeKon nicht nur rechtlich bestehen, sondern im Zweifel tatsächlich durchgesetzt werden können.

¹³² Wetzling, Bedingt kontrollfähig, S. 22 f.

¹³³ Wetzling, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 9.

¹³⁴ Vgl. [Teil 3 C. IX. 2.](#)

¹³⁵ Fahrner begründet die Notwendigkeit von Minderheitenrechten zusätzlich mit der Gerichtsähnlichkeit der Kontrolle Fahrner, GSZ 2023, 223, 226 f.

¹³⁶ Fahrner, GSZ 2023, 223, 226.

(1) Durchsetzung der Kontrollmittel und Schutz gegen Falschaussagen

Im Gesetzgebungsverfahren zum BNDG wurde wiederholt darauf hingewiesen, dass der UKRat jedenfalls gegenüber Externen über keinerlei Durchsetzungsinstrumente verfügt und dass ihm gegenüber getätigte Falschaussagen folgenlos bleiben.¹³⁷

Um diese Defizite zu beheben, muss das GeKon die Möglichkeit haben, seine Kontrollmittel gem. § 56 BNDG durchzusetzen. Daher sollte erstens das Beweisrecht der VwGO oder das der StPO im neuen UKRatsG für analog anwendbar erklärt werden.¹³⁸

Zweitens sollten uneidliche Falschaussagen gegenüber dem GeKon zukünftig strafbar sein. Dafür spricht, dass das GeKon ansonsten gegen Falschaussagen schlechter geschützt ist als „ein normales Gericht oder ein Parlamentarischer Untersuchungsausschuss“ (§§ 153 StGB, 162 Abs. 2, 153 StGB), obwohl diese Informationen für die Aufgabenerfüllung durch das GeKon von zentraler Bedeutung sind.¹³⁹ Eine Lösung könnte darin bestehen, dass der Wortlaut von § 162 Abs. 2 StGB so angepasst werden, dass das GeKon davon erfasst ist.¹⁴⁰

(2) Durchsetzung gegenüber dem Nachrichtendienst und der Aufsichtsbehörde

Darüber hinaus zwingen die Erfahrungen im Umgang der Exekutive mit der G 10-Kommission dazu, zu überlegen, was im Fall des „Kompetenz-Konflikts“¹⁴¹ passiert: Der G 10-Kommission wurde die Einsicht in Selektoren verwehrt, obwohl ihr eigentlich uneingeschränkte Kontrollmittel zustehen. Dagegen konnte sie sich mangels alternativem Rechtsweg nur vor dem Bundesverfassungsgericht wehren, was erfolglos blieb, weil ihre Parteifähigkeit im Organstreit verneint wurde.¹⁴²

¹³⁷ Vgl. [Teil 3 C. VIII. 2. c.](#), bei Mitarbeitern der Nachrichtendienste kann sich das GeKon demgegenüber an die Präsidenten der Nachrichtendienste wenden, die ihren Mitarbeitern dann eine entsprechende Weisung zur Aussage erteilen müssten, *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12.

¹³⁸ Zur Auskunftspflicht beispielsweise (§§ 96 Abs. 1, 98 VwGO, §§ 355 ff., 380, 390, 409 ZPO), *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12; schlagen als weitere Alternative die Anwendung des Parlamentarischen Untersuchungsausschussgesetzes (§§ 27, 29 Abs. 3 PUAG) vor, *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 23.

¹³⁹ *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 12.

¹⁴⁰ De lege feranda könnte § 162 Abs. 2 StGB beispielsweise so lauten: „Die §§ 153 und 157 bis 160, soweit sie sich auf falsche uneidliche Aussagen beziehen, sind auch auf falsche Angaben vor einem Untersuchungsausschuss eines Gesetzgebungsorgans des Bundes oder eines Landes und vor dem *Gerichtsähnlichen Kontrollorgan des Bundes* anzuwenden.“

¹⁴¹ Graulich verwendet den Begriff im Zusammenhang mit der Frage, was beispielsweise bei „Meinungsverschiedenheiten“ über den Umfang des Tätigkeitsberichts an das PKGr geschehe, *Graulich*, GSZ 2021, 121, 129.

¹⁴² Vgl. [Teil 3 B. XII. 2.](#); BVerfG, Beschluss v. 20.9.2016 - 2 BvE 5/15.

Für den Fall, dass die Nachrichtendienste bzw. ihre Aufsichtsbehörden einem Kontrollbegehren des GeKon nicht nachkommen oder Meinungsverschiedenheiten über die Verfügungsberechtigung des BND¹⁴³ auftreten, stünde das GeKon vor dem gleichen Problem wie die G 10-Kommission, weil das geltende Recht hierfür keine Vorkehrungen trifft. Da Kontrollbefugnisse nur „wirksam“ sind, wenn der beabsichtigte Erfolg tatsächlich eintritt, sind die Kontrollmittel des GeKon dann in verfassungswidriger Weise unwirksam.

Zur Lösung dieses Problems bei der Kontrolle von Nachrichtendiensten schlug *Masing* vor, zu überlegen, ob Kontrollmittel nicht „gerichtlich durchsetzbar ausgestaltet sein sollten“. Die Kontrolle könne „selbst nicht im Wesentlichen an Gerichte delegiert werden. Das hindere aber nicht darüber nachzudenken, ob dann nicht zumindest Kontrollbefugnisse ihrerseits durch Klage- und Antragsbefugnisse wirksam unterstützt werden können, um nicht zahnlos zu werden“.¹⁴⁴

Dem ist zuzustimmen, denn die Wirksamkeit der Kontrollmittel kann nach den praktischen Erfahrungen der G 10-Kommission nur sichergestellt werden, wenn ein Gericht eingebunden werden kann, das den Nachrichtendienst bzw. die Aufsichtsbehörde im Zweifel dazu verpflichtet, dem Kontrollbegehren nachzukommen. Zu diesem Zweck sollte dem GeKon daher eine Klagebefugnis zum Bundesverwaltungsgericht verliehen werden. Auf diese Möglichkeit sollte das GeKon nur als ultima ratio zurückgreifen, um zu verhindern, dass die Kontrolle auf das Gericht verlagert wird.

Beim Bundesverwaltungsgericht sollte ein Fachsenat für die Überprüfung nachrichtendienstlicher Maßnahmen eingeführt werden, in dem die Verfahren *in-camera* unter Wahrung der notwendigen Geheimhaltungsvorkehrungen stattfinden (vgl. §§ 189 i. V. m. 99 Abs. 2 VwGO)¹⁴⁵. Ein entsprechender Fachsenat wurde in der Literatur zwar mehrfach gefordert, allerdings sollte das Bundesverwaltungsgericht nach diesen Überlegungen als eigentlicher Kontrolleur tätig werden, der über die Rechtmäßigkeit der nachrichtendienstlichen Tätigkeit entscheidet.¹⁴⁶ In dem hier vorgeschlagenen Modell

¹⁴³ Vgl. [Teil 3 C. VIII. 2. a.](#)

¹⁴⁴ *Masing*, Nachrichtendienste, 3, 14.

¹⁴⁵ *Graulich*, Justizgewährung und Geheimdienste, 143, 161; *Bantlin*, G 10-Kommission, S. 232 ff.; *Riegel*, DöV 1985, 435; verweist darauf, dass Geheimhaltungsbedenken „im Rahmen der einschlägigen prozessrechtlichen Vorschriften über den Ausschluss der Öffentlichkeit und über die Einschränkung der Pflicht zur Vorlage der Akten (§ 99 VwGO) Rechnung getragen werden.“, *Deiseroth*, ZRP 2013, 196.

¹⁴⁶ Antragsberechtigt sollen in dem Modell „nach dem Vorbild des Verbandsklagerechts“ Fraktionen oder „zu benennende Quoren des Parlaments“ sein, die geltend machen, ein Nachrichtendienst habe „bei einer bestimmten Handlungsweise seinen Ermächtigungsrahmen nicht eingehalten, also objektives Recht verletzt“, *Graulich*, Justizgewährung und Geheimdienste, 143, 161 f.; antragsberechtigt soll in diesem Modell die G 10-Kommission sein, *Bantlin*, G 10-Kommission, S. 232 ff.; fordert auch gerichtliche Kontrollen *Riegel*, DöV 1985, 435.

würde der Fachsenat im Fall eines Kompetenz-Konflikts lediglich über die Kontrollmittel entscheiden, die eigentliche Kontrolle und die Feststellung der Kontrollergebnisfolgen blieben Aufgabe des GeKons.

f. Kontrollergebnisfolgen

Das GeKon entscheidet über ihm vorgelegte Sachverhalte abschließend.¹⁴⁷ Die Art und Weise wie diese Entscheidungen ergehen, sollte gesetzgeberisch näher ausgestaltet werden (aa)). Außerdem sollten die Regelungen zur Kooperation mit dem Parlamentarischen Kontrollgremium überarbeitet werden (bb)).

aa) Genehmigungsentscheidung

Die Entscheidungen des GeKon sollten stets begründet (1) und die Begründung bei fallübergreifend bedeutenden Entscheidungen veröffentlicht werden (2). Außerdem sollten Mitglieder des GeKon die Möglichkeit haben, Sondervoten zu veröffentlichen (3).

(1) Begründungspflicht für Entscheidungen

Während der UKRat eine ablehnende Entscheidung stets begründet, muss er stattgebende Entscheidungen gem. § 12 VerfO-UKRat nicht begründen. In der Praxis begründet er offenbar teilweise auch stattgebende Entscheidungen, wenn sie „rechtsfortbildende[n] oder richtungsweisende[n] Inhalt“ haben.¹⁴⁸

Zukünftig sollten alle Entscheidungen des GeKon begründungspflichtig sein.¹⁴⁹ Wenn ablehnende Entscheidungen begründungspflichtig sind, sollten es stattgebende erst recht sein, weil sie es sind, die Grundrechtseingriffe zur Folge haben.

Zudem spricht für eine generelle Begründungspflicht, dass die durch das GeKon genehmigten Anordnungen für die sich ggf. daran anschließenden Kontrollen des BfDI von Bedeutung sein können. Das Einsichtnahmerecht des BfDI erstreckt sich auf die Genehmigung der Datenerhebung, weil er nur so die Einhaltung etwaiger Anordnungsvoraussetzungen prüfen kann. Hilfreich ist die Einsichtnahme der Genehmigung nur dann, wenn die Kontrolleure des BfDI die rechtlichen Erwägungen des GeKon nachvollziehen können.

Außerdem könnte die Begründungspflicht dazu beitragen, dass vergleichbare Sachverhalte auch vergleichbar beschieden werden. Durch die Begründungspflicht ließe sich

¹⁴⁷ Vgl. [Teil 3 C. IX. 1.](#)

¹⁴⁸ *Hoch/Schmidt-Räntsch/Brunst*, NVwZ 2023, 712, 716.

¹⁴⁹ *Fahrner*, GSZ 2023, 223, 224; *Wetzling*, Bedingt kontrollfähig, S. 24.

zudem verhindern, dass Anordnungen nach einer „nur pauschalen Überprüfung einfach gegengezeichnet werden.“¹⁵⁰ Das gelingt nur, wenn die Begründungen selbst detailliert und aussagekräftig sind.

(2) Veröffentlichung von Entscheidungsgründen

Soweit es aus Geheimhaltungsgründen realisierbar ist, sollten Entscheidungen des GeKon veröffentlicht werden. Auf diese Weise kann das Vertrauen in die Arbeit der Behörde gestärkt¹⁵¹ und eine wissenschaftliche Auseinandersetzung und öffentliche Debatte ermöglicht werden¹⁵². Dass dies trotz verständlicher Geheimhaltungsbedürfnisse realisierbar ist, zeigt die Praxis in anderen Staaten, in denen Entscheidungen bereits in Teilen veröffentlicht werden.¹⁵³

Allerdings sollte nicht jede einzelne Entscheidung veröffentlicht werden, um im Interesse der Nachrichtendienste und der Sicherheit zu verhindern, dass die Anzahl der Anordnungen öffentlich nachvollziehbar wäre. Stattdessen ist es für die genannten Zwecke ausreichend, wenn Entscheidungen nur veröffentlicht werden, die von besonderer Bedeutung sind, weil sich daraus beispielsweise die Auslegung eines unbestimmten Tatbestandsmerkmals oder eine Rechtsprechungsänderung ergeben. Bereits ergangene Entscheidungen sollten ebenfalls veröffentlicht werden, wenn sie fallübergreifend wichtig sind, damit die bisherige Gesetzesauslegung nachvollzogen werden kann.

(3) Möglichkeit zu Sondervoten

Einzelne Mitglieder des GeKon sollten die Möglichkeit haben, ihre abweichende Position zur Mehrheitsentscheidung in einem Sondervotum darzulegen¹⁵⁴, das dann zusammen mit der Entscheidung veröffentlicht wird. Da der unabhängige Vorabkontrollleur über beträchtliche Macht verfügt und wegen seiner Unabhängigkeit nicht kontrolliert wird, sind Minderheitenrechte von zentraler Bedeutung.¹⁵⁵ Das Sondervotum wäre ein besonders wirksames Minderheitenrecht, denn schon die Möglichkeit es zu nutzen, würde die Diskurs- und Kompromissbereitschaft der Gremienmehrheit erhöhen. Wenn die Sondervoten mit der Entscheidung veröffentlicht werden, würden sowohl die Öffentlichkeit als auch die Wissenschaft und Politik über die zugrundeliegende Problematik informiert und könnten darauf reagieren.

¹⁵⁰ Fahrner, GSZ 2023, 223, 224.

¹⁵¹ Venedig-Kommission, Report 2015, S. 52 Rn. 238.

¹⁵² Hoch/Schmidt-Räntsch/Brunst, NVwZ 2023, 712, 716.

¹⁵³ Mit Verweis auf das zuständige niederländischen Gremium, Wetzling/Vieth, Mehr Rechtskontrolle wagen, S. 21, Wetzling, Bedingt kontrollfähig, S. 16.

¹⁵⁴ Wetzling, Bedingt kontrollfähig, S. 23.

¹⁵⁵ Fahrner, GSZ 2023, 223, 227; vgl. [Teil 2 A. IV. 2. d.](#)

Gegen die Einführung von Sondervoten wird vor allem vorgebracht, dass diese die richterliche Unabhängigkeit, genauer das Beratungsgeheimnis, verletzen.¹⁵⁶ Das Beratungsgeheimnis soll verhindern, dass einzelne Mitglieder sich vor „Reaktionen und Gängelungen“ in der Öffentlichkeit oder durch die Justizverwaltung fürchten müssen, weil Details aus den Beratungen bekannt geworden sind.¹⁵⁷ *Fabrner* weist darauf hin, dass diese Nachteile nur dann eintreten, wenn das Sondervotum öffentlich bekannt wird.¹⁵⁸ Deshalb schlägt er vor, das Sondervotum wenigstens intern zu dokumentieren, um wegen der „persönlichen Verantwortlichkeit“ und „der persönlichen individuellen Rechtsstaatsbindung“ zu verhindern, dass einzelne Mitglieder von Mehrheitsentscheidungen „vereinnehm und für diese persönlich haftbar“ gemacht werden.¹⁵⁹ Dieser Vorschlag hätte den Nachteil, dass die Information der Öffentlichkeit vorenthalten würde und eine Lösung des zugrundeliegenden Problems damit unwahrscheinlicher wird. Wenn das Sondervotum nicht veröffentlicht werden soll, müsste es – unter Wahrung der notwendigen Geheimhaltungsvorkehrungen – daher zumindest dem Parlamentarischen Kontrollgremium zugänglich gemacht werden.¹⁶⁰

Bei der Erörterung der Vor- und Nachteile der Offenlegung von Sondervoten ist zu bedenken, dass sich die Sondervoten nur auf einzelne Aspekte beziehen, in denen die Autoren eine andere Meinung vertreten und deshalb der Beratungsverlauf überwiegend geheim bleibt. Im Ergebnis kommt es nur zu einer geringfügigen Beeinträchtigung des Beratungsgeheimnisses, was vor dem Hintergrund der mit der Veröffentlichung des Sondervotums verbundenen Vorteile allerdings hinnehmbar erscheint.

bb) Austausch mit dem Parlamentarischen Kontrollgremium

Dass das GeKon sich mit dem Parlamentarischen Kontrollgremium austauscht, ist eine weitere Kontrollergebnisfolge. Dabei geht es anders als bei der Genehmigung in der Regel nicht um einzelne Vorgänge, sondern darum, strukturelle Probleme politisch zu lösen.¹⁶¹ Die Kooperation mit dem Parlamentarischen Kontrollgremium sollte zukünftig in einer Norm geregelt sein (1.). Darüber hinaus sollte die Norm zur Berichterstattung überarbeitet werden (2.).

¹⁵⁶ Zum Sondervotum: „Und auch der Kontrollrat lehnt das ab. Erheblicher Mehraufwand und vielfältige Probleme wie das Unterlaufen des Beratungsgeheimnisses und Rechtsunsicherheit bei den BND-Mitarbeitern könnten Folgen sein“, *Banse et al.*, Das Kreuz mit der Kontrolle.

¹⁵⁷ *Fabrner*, GSZ 2023, 223, 226.

¹⁵⁸ *Fabrner*, GSZ 2023, 223, 226.

¹⁵⁹ *Fabrner*, GSZ 2023, 223, 226.

¹⁶⁰ *Wetzling*, Bedingt kontrollfähig, S. 25; ein Sondervotum an das PKGr sah offenbar auch der Entwurf zu einem UKRats-G vor, *Banse et al.*, Das Kreuz mit der Kontrolle.

¹⁶¹ Vgl. [Teil 3 C. IX. 3.](#)

(1) Separate Norm zur Kooperation mit dem UKRat

Aktuell sind die Regelungen über die Zusammenarbeit zwischen dem UKRat und dem Parlamentarischen Kontrollgremium auf zwei Normen verteilt (§§ 55, 58 Abs. 1 BNDG). Die Vorgaben zur Kooperation mit dem Parlamentarischen Kontrollgremium sollten zukünftig separat geregelt werden, das heißt, sie sollten von den Vorgaben zur Zusammenarbeit mit den anderen Rechtskontrolleuren getrennt werden. Dafür sprechen systematische Gründe, weil das Parlament als „Dritter“ im Sinne der Third Party Rule gilt.

Die Regelung gem. § 58 Abs. 1 BNDG, wonach sich die beiden Gremien über allgemeine Angelegenheiten austauschen können, sollte daher in der neuen Kooperationsnorm im Kontrollratsgesetz ergänzt und in § 58 BNDG gestrichen werden.

(2) Berichterstattung gegenüber dem Parlamentarischen Kontrollgremium

De lege lata berichtet der UKRat dem Parlamentarischen Kontrollgremium im Abstand von höchstens sechs Monaten von seiner Tätigkeit (§ 55 Abs. 1 BNDG). Dieser Zeitraum sollte unter anderem vor dem Hintergrund der Aufgabenausweitung des UKRat auf maximal drei Monate verkürzt werden.¹⁶²

Allerdings darf der Austausch nicht so weit gehen, dass das PKGr alle Tätigkeiten des UKRats nachvollziehen und überprüfen kann, denn dann droht eine Verletzung der Third Party Rule. Gegen einen zu engen Austausch sprechen die hinter der Rechtskontrolle stehenden Überlegungen, die gerade „auf Effektivierung durch Entpolitisierung“ setzen.¹⁶³

Andererseits darf eine so mächtige Behörde wie der UKRat in einem Rechtsstaat schon aus Legitimationsgründen¹⁶⁴ nicht völlig kontrollfrei agieren. Dass nur die Exekutive in Form der Aufsichtsbehörden der Nachrichtendienste das GeKon kontrolliert, ist keine Option, weil die Unabhängigkeit von ihnen zwingende Voraussetzung einer verfassungskonformen und konventionskonformen externen Kontrolle ist. Die Berichtspflicht gegenüber dem Parlamentarischen Kontrollgremium bietet hier einen Mittelweg: Einerseits ist der UKRat in der Pflicht, seine Tätigkeit zu erklären, andererseits muss er nicht über alle seine Tätigkeiten berichten und kann darauf achten, dass

¹⁶² Anders sieht dies die Mehrheit der Mitglieder des GeKons, laut ihrem Gesetzesentwurf sollen die Berichte nur noch „in der Regel“ einmal jährlich erfolgen, § 28 Abs. 1, *Hoch et al.*, Diskussionsentwurf, S. 12.

¹⁶³ *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 14 f.; *Barczak*, KritV 2021, 91, 129.

¹⁶⁴ Vgl. Teil 2 A. IV. 2. c.; „If the problem for parliamentary accountability bodies can be summarized in the word ‘competence’, the problem for expert bodies can be summarized in the word ‘legitimacy’ (...) Moreover, in order to maintain parliament’s confidence in the expert body it is necessary to provide for institutional links between the two.“, *Venedig-Kommission*, Report 2015, S. 51 Rn. 231.

die Third Party Rule nicht verletzt wird. Wo eine Verletzung der Third Party Rule allerdings nicht zu befürchten ist, muss das GeKon dem Parlamentarischen Kontrollgremium umfassend Bericht erstatten.

Zudem sollte das PKGr – ebenfalls unter Wahrung der Third Party Rule – die Möglichkeit haben, detaillierte Berichte zu bestimmten Aspekten anzufordern. Es wäre außerdem sinnvoll, dem PKGr die Möglichkeit zu geben, das GeKon zu einzelnen Kontrollen einzuladen, um dessen Expertise nutzen zu können.

Falls die fallübergreifend relevanten Entscheidungen des GeKon – entgegen dem hier formulierten Vorschlag¹⁶⁵ – (auch) zukünftig nicht veröffentlicht werden, müssen sie zumindest im Bericht für das PKGr enthalten sein.¹⁶⁶

Dass die im Vierteljahresrhythmus erteilten Berichte einen vollständigen Überblick über die Tätigkeit des GeKons verschaffen müssen, dass das PKGr spezifische Berichte anfordern kann und die Mitglieder des GeKons theoretisch an Kontrollen des Parlamentarischen Kontrollgremiums teilnehmen können, sollte in der neuen Kooperationsnorm ergänzt werden.¹⁶⁷

g. Fachkompetenz und Ressourcen

Da dem GeKon nach diesem Modell mit der Vorabkontrolle weiterer Befugnisse zusätzliche Aufgaben übertragen wurden, muss dessen Mitglieder- und Mitarbeiteranzahl erhöht werden. Darüber hinaus sollte das GeKon die Möglichkeit haben, sich im Einzelfall externen (technischen) Sachverstand einzuholen.¹⁶⁸ Im Mitarbeiterstab des GeKon sollten IT-Experten angestellt werden, auf deren Sachverstand laufend zurückgegriffen werden kann.¹⁶⁹

¹⁶⁵ Vgl. [Teil 4 B I. 3. f. aa. \(2\)](#).

¹⁶⁶ Fordert eine umfangreichere Information des PKGr über „Entscheidungen und Leitsätze bei der Auslegung des Nachrichtendienstrechts (...)“; *Wetzling*, Bedingt kontrollfähig, S. 17.

¹⁶⁷ Die Möglichkeit, das GeKon bei Kontrollen des PKGr hinzuzuziehen, müsste auch im PKGrG ergänzt werden.

¹⁶⁸ *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 22; Bert Hub, ein Mitglied des niederländischen Kontrollorgans, begründet seinen Rücktritt jedoch unter anderem damit, dass jedenfalls die niederländischen Kontrolleure Probleme hatten, überhaupt technische Experten zu rekrutieren: “In the current labor market, it is unlikely that a regulator will be able to swiftly recruit sufficient numbers of highly skilled computer experts able to do ongoing investigations of sophisticated hacking campaigns and bulk interception projects“, *Hubert*, On my resignation as regulator of the Dutch intelligence and security services.

¹⁶⁹ Der „Kontrollperson“ müssten auch „eigene Mitarbeiter“ zur Verfügung stehen, die sie dabei unterstützen, die anspruchsvollen Vorgänge „wirklich zu durchdringen“, *Fabrner*, GSZ 2023, 223, 225.

Es muss sichergestellt sein, dass die Mitglieder des GeKon die Materie so durchdringen, dass die „Wirksamkeit“ der Kontrolle „nicht kraft überlegenen Wissens der vorlegenden Stelle überspielt“ wird.¹⁷⁰

4. Datenschutzkontrolle durch den BfDI

Bei einer Reform der Rechtskontrolle der Nachrichtendienste des Bundes sollten die verfassungsrechtlichen Defizite bei der Kontrolle durch den BfDI¹⁷¹ behoben werden. Während die Zuständigkeit des BfDI für die Kontrolle unverändert bleiben sollte, müsste der Kontrollgegenstand um einen Aspekt ergänzt werden (a.), das Kontrollintervall gesetzlich verkürzt (b.), die Kontrollmittel und -ergebnisfolgen verstärkt (c., d.) und die Kontrollbarrieren abgebaut werden (e.).

a. Kontrollgegenstand

Bereits nach geltendem Recht muss der BfDI beim Erlass von Dateianordnungen angehört werden, um bereits bei der Errichtung automatisierter Dateien „verfahrenstechnische und verfahrensrechtliche Schranken“ vorsehen zu können, die verhindern, dass die Daten „über das für die Aufgabenerfüllung erforderliche Maß“ verwendet werden.¹⁷² In der Norm sollte zukünftig klargestellt werden, dass der BfDI zusätzlich immer einzubinden ist, wenn (im Rahmen von bestehenden Dateianordnungen) neue automatisierte oder gar selbstlernende Systeme eingesetzt werden sollen. So lässt sich absichern, dass diese Anwendungen unterbleiben, wenn es dafür nach der neuesten Verfassungsrechtsprechung einer speziellen Rechtsgrundlage bedürfte¹⁷³. Falls eine Rechtsgrundlage dafür geschaffen wird, könnte der BfDI somit sicherstellen, dass sie beachtet wird.

b. Modalität

Das Bundesverfassungsgericht fordert ein „regelmäßiges“ Intervall von maximal zwei Jahren zwischen den Stichprobenkontrollen.¹⁷⁴ Weil die Datenschutzkontrolle für die Verhältnismäßigkeit der Eingriffe von entscheidender Bedeutung ist, sollten die Vorgaben des Bundesverfassungsgerichts gesetzlich abgebildet werden, um die Entscheidung über die (Mindest-)Anzahl der Stichprobenkontrollen nicht der Datenschutzbehörde

¹⁷⁰ *Fahrner*, GSZ 2023, 223, 225.

¹⁷¹ Vgl. ab. [Teil 3 D. II. 3.](#)

¹⁷² Vgl. [Teil 3 D. II. 1. d.](#); § 14 Abs. 1 S. 2 BVerfSchG, § 8 MADG, § 8 BNDG; [Bt-Drs. 11/4306](#), Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 6.4.1989, S. 62; Schenke/Graulich/Ruthig/Mallmann, § 14 BVerfSchG Rn. 2.

¹⁷³ Vgl. [Teil 1 B. III. 1. a.](#)

¹⁷⁴ Vgl. [Teil 2 A. III. 1. a. ee\).](#)

zu überlassen¹⁷⁵. Das vom Bundesverfassungsgericht gewählte Intervall von maximal zwei Jahren zwischen zwei Kontrollen ist zu weit bemessen. Es erkennt die zentrale Bedeutung der Kontrolle durch die Datenschutzbeauftragten für die Wahrung der Verhältnismäßigkeit von heimlichen Datenverarbeitungen – gerade im Nachrichtendienstrecht¹⁷⁶.

Auf der anderen Seite darf der durch die Kontrollen bedingte Aufwand für die Nachrichtendienste nicht zu hoch werden. Hier muss angemerkt werden, dass von der jeweiligen Stichprobenkontrolle in der Regel nur einzelne Abteilungen betroffen sein werden, sodass nicht dem gesamten Nachrichtendienst Mehraufwand entsteht. Als Mindestkontrollintervall sinnvoll erscheint je nach Umfang der Kontrolle ein Zeitraum von maximal drei Monaten zwischen zwei Stichprobenkontrollen. Zur genauen Festlegung des Intervalls sollte der Gesetzgeber den Sachverstand und die Erfahrungswerte der Kontrolleure und Kontrollierten einholen. Darüber hinaus wäre es auch empfehlenswert, den Datenschutzkontrolleuren (unter Wahrung notwendiger Geheimhaltungsschranken) einen direkten Zugriff auf einzelne Datenbanken einzuräumen, sodass sie jederzeit Einblick nehmen können, ohne dass dem Nachrichtendienst Mehrarbeit entsteht.¹⁷⁷

Ein gesetzlich kürzer gefasstes Mindestkontrollintervall hätte den Vorteil, dass der Gesetzgeber sicher davon ausgehen kann, dass ein definierter Kontrollabstand nicht unterschritten wird. Nichtsdestotrotz bliebe den Datenschutzbeauftragten genügend Spielraum, ihre Kontrollen im Bedarfsfall noch enger zu gestalten.

Unabhängig von den gesetzlichen Regelungen sollte in der Praxis darüber nachgedacht werden, die Kontrolle zu automatisieren. Dann könnten die Datenschutzkontrolleure beispielsweise automatisch informiert werden, wenn Nachrichtendienste Daten an ausländische Stellen übermitteln, sodass sie wissen, was sie nachträglich kontrollieren können¹⁷⁸.

Eine lückenlose nachträgliche Kontrolle wird dennoch nicht möglich sein. Sie wäre aber auch nicht wünschenswert, weil die „grundsätzliche Lückenhaftigkeit der Kon-

¹⁷⁵ Vgl. [Teil 3 D. II. 3.](#)

¹⁷⁶ Vgl. [Teil 2 A. IV. 2. b. cc\).](#)

¹⁷⁷ *Wetzling/Vieth* weisen unter anderem darauf hin, dass Kontrolleure in anderen europäischen Staaten über einen solchen direkten Zugriff auf Datenbanken verfügen. Sie können „sich in die technischen Systeme der Nachrichtendienste einloggen und vollkommen unabhängig Daten ihrer Wahl abrufen und auswerten.“ Der direkte Zugriff bedeute jedoch nicht, dass ein „vollständige Zugriff“ vorgesehen sei. Gewisse Grenzen seien aus Sicherheits- und Geheimhaltungsgründen vermutlich notwendig, *Wetzling/Vieth*, Datenbasierte Nachrichtendienstkontrolle, S. 14.

¹⁷⁸ *Wetzling/Vieth*, Datenbasierte Nachrichtendienstkontrolle, S. 3 ff. Die zitierte Ausarbeitung bietet viele sinnvolle Anregungen, wie die Kontrolle in der Praxis effektiert werden kann.

trolle“ Maßstab von Rechtsstaatlichkeit ist, indem sie verhindert, dass „repressiven Elemente von Kontrolle in dysfunktionaler Weise“ übersteigert werden. Lückenlose Kontrolle ist nicht notwendig, weil bereits die Möglichkeit von Kontrollen das Verhalten des Kontrollierten beeinflusst.¹⁷⁹

c. Initiative

Bereits nach geltendem Recht haben potenziell Betroffene das Recht, sich mit Beschwerden an den BfDI zu wenden (§ 28 Abs. 1 BVerfSchG). Man kann deshalb erwägen, an Stelle des GeKon den BfDI als Kontrolleur auf der dritten Stufe vorzusehen, um die Rechtsprechung des EGMR umzusetzen. Im Ergebnis liegt es jedoch näher, das GeKon damit zu beauftragen, denn auch der BfDI ist (wie das GeKon) für Kontrollen auf einer weiteren Stufe zuständig, wird anders als das GeKon jedoch nicht durch eine weitere Institution überprüft. Deshalb besteht die Gefahr, dass der EGMR die ex post Kontrolle durch den BfDI mit Verweis auf seine Rechtsprechung in *Rättvisa gg. Schweden* wegen Interessenskonflikten¹⁸⁰ als unzureichend bemängeln würde.

Falls der ex post-Rechtsbehelf Betroffener dennoch an den BfDI adressiert werden soll, wäre dies nur konventionskonform, wenn der BfDI – im Einklang mit dem hier formulierten Vorschlag – bindende Entscheidungen treffen könnte.¹⁸¹ Darüber hinaus müssten auch seine Entscheidungen mindestens gegenüber einem sicherheitsüberprüften Betroffenenanwalt begründet werden.¹⁸²

d. Stärkung der Kontrollmittel des BfDI

Wie schon bei den Kontrollmitteln des GeKons ist auch bei den Kontrollmitteln des BfDI problematisch, dass sie im Zweifel gegenüber der Exekutive nicht durchgesetzt werden können. Um dies zu verhindern, muss auch dem BfDI eine Klagebefugnis an den zu schaffenden Fachsenat des Bundesverwaltungsgerichts verliehen werden, auf die er als ultima ratio zurückgreifen kann.

Darüber hinaus ist es für die Wirksamkeit der Kontrollen des BfDI von zentraler Bedeutung, dass sein Bild des Ist-Zustands der Realität entspricht. Deshalb müssen Falschaussagen – wie beim Vorschlag für den UKRat – auch ihm gegenüber strafbar sein. Der BfDI sollte insoweit auf keinen Fall schlechter gestellt sein als das GeKon,

¹⁷⁹ Hoffmann-Riem, Verwaltungskontrolle, 433, 354.

¹⁸⁰ Vgl. Teil 2 B. I. 4. b. ff).

¹⁸¹ Vgl. Teil 3 D. II. 6. c., s.u. Teil 4 B. I. 4. e. aa).

¹⁸² Vgl. Teil 4 B. I. 3. f. aa) (1).

denn seine Kontrollen sind nicht weniger wichtig als die gerichtsähnlichen Vorabkontrollen. Im Gegenteil können manche Kontrollzwecke sogar durch laufende und nachträgliche Kontrollen besser verwirklicht werden als bei der Vorabkontrolle¹⁸³.

e. Stärkung der Kontrollergebnisfolgen des BfDI

Die Kontrollergebnisfolgen des BfDI sollten erweitert werden.

aa) Anordnungsbefugnis

Die Beanstandung ist keine „wirksame“ Befugnis im Sinne der Rechtsprechung¹⁸⁴. Der BfDI sollte deshalb gegenüber dem Nachrichtendienst dazu befugt sein, als ultima ratio den Abbruch rechtswidriger Datenverarbeitungen und die Löschung von rechtswidrig erlangten Daten anzuordnen.¹⁸⁵ Als Regelungsvorbild dafür kommt § 69 Abs. 2 BKAG in Betracht, wonach der BfDI „geeignete Maßnahmen“ anordnen kann, wenn dies für die Beseitigung eines „erheblichen“ Verstoßes gegen das Datenschutzrecht erforderlich ist.¹⁸⁶ Letztlich gibt es keinen überzeugenden Grund, wieso die Kontrolle des BfDI weniger durchschlagend sein sollte als die des GeKons und der G 10-Kommission, die über ein abschließendes Entscheidungsrecht verfügen¹⁸⁷. Was für diese Kontrolleure als notwendig erachtet wird, gilt für den BfDI ebenso. Offenbar gibt es die Befürchtung, die Tätigkeit der Nachrichtendienste könne durch eine ungerechtfertigt weitgehende Nutzung des Anordnungsrechts durch den BfDI zu sehr behindert werden. In diesem Zusammenhang wäre es interessant, die Perspektive des BKAs über die tatsächlichen praktischen Konsequenzen von § 69 Abs. 2 BKAG einzuholen.

Den möglichen Befürchtungen, dass die Tätigkeit der Nachrichtendienste durch Anordnungen des BfDI ungerechtfertigt beeinträchtigt würde, könnte man mit flankierenden Mechanismen begegnen. So könnte etwa der BfDI verpflichtet werden, das PKGr – unter Wahrung der Third Party Rule¹⁸⁸ – vorab substantiiert über seine An-

¹⁸³ Vgl. [Teil 2 A. IV. 2. b.](#)

¹⁸⁴ Vgl. [Teil 3 D. II. 6. c.](#)

¹⁸⁵ *Sosna*, GSZ 2022, 245, 247; *BfDI*, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 11; fordern „Sanktionsbefugnisse“, *Wetzling/Moßbrucker*, BND-Reform, die Zweite, S. 47; verweist darauf, dass dies in einigen europäischen Ländern bereits so gehandhabt wird, *Ruckerbauer*, Stärkung des Datenschutzbeauftragten, S. 6.

¹⁸⁶ *BfDI*, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 11; fordert außerdem, die Fachaufsicht dazu zu verpflichten, dem BfDI innerhalb von vier Wochen zu berichten, „wie diese Abhilfemaßnahmen umgesetzt worden sind“, *Ruckerbauer*, Stärkung des Datenschutzbeauftragten, S. 5.

¹⁸⁷ Vgl. [Teil 3 C. IX. 1.](#), [Teil 3 B. IX.](#)

¹⁸⁸ Vgl. die Unterrichtung des UKRat [Teil 3 C. IX. 3.](#)

ordnungen und deren Begründung zu unterrichten. Dadurch entstünde eine rationalisierende Erklärungspflicht. Als positiver Nebeneffekt werden die Abgeordneten über Defizite informiert, sodass sie bei Bedarf gesetzlich nachsteuern können.

Zur „finalen Klärung“ einer Streitigkeit zwischen dem Nachrichtendienst und dem BfDI wird vorgeschlagen, einen „besondere[r] Rechtsweg“ zu etablieren.¹⁸⁹ Hierfür sollte der bereits vorgeschlagene Fachsenat beim Bundesverwaltungsgericht zuständig sein.¹⁹⁰ Dies würde sowohl dem betroffenen Nachrichtendienst als auch dem BfDI die Möglichkeit geben, ihre Standpunkte vor einem neutralen Dritten erörtern zu können und Streitigkeiten nach der Entscheidung durch das Gericht beilegen zu können. Sieht man eine solche Möglichkeit zur Klärung einer ausweglosen Situation nicht vor, könnte ein von Misstrauen geprägtes Verhältnis zwischen Kontrolleur und Kontrolliertem entstehen, was letztlich einer wirksamen Kontrolle schadet.¹⁹¹

Wegen dem mit dem Rechtsweg zum Bundesverwaltungsgericht verbundenen Aufwand und Zeitverlust kommt dieses Instrument nur als ultima ratio in Betracht.

bb) Einzelfallberichterstattung gegenüber dem PKGr

De lege lata tauschen sich die Kontrolleure nur über „allgemeine Angelegenheiten“ aus (§ 58 Abs. 3 BNDG, § 15 Abs. 1 PKGrG¹⁹²). Der BfDI und das PKGr sollten ermächtigt werden, sich – unter Wahrung der Third Party Rule – zudem über einzelne Sachverhalte und Dateiverarbeitungen bzw. -programme auszutauschen.¹⁹³ Der BfDI sollte außerdem dazu verpflichtet werden, das PKGr zu unterrichten, soweit er rechtswidrige Zustände identifiziert, denen nicht abgeholfen wird.

f) Abbau von Barrieren

Darüber hinaus müssen die Kontrolltätigkeit des BfDI beeinträchtigende rechtliche Kontrollbarrieren abgebaut (aa)) und Ressourcenbarrieren verhindert (bb)) werden.

¹⁸⁹ *Sosna*, GSZ 2022, 245, 247; „Besäßen die Datenschutzbeauftragten rechtliche Sanktions- und Durchsetzungsmacht, dann müßten die Entscheidungen dieser Institution gemäß dem Prinzip der Gewaltenteilung selbst wiederum durch andere, justizielle Kontrollorgane überprüft werden können, um in den Datenschutzkontrollinstanzen eine zweite, der Stellung des Bundesverfassungsgerichts vergleichbare und neben diesem in Frage des Datenschutzes konkurrierende oberste Kontrollbehörde zu vermeiden“, *Kauß*, *Der suspendierte Datenschutz*, S. 406.

¹⁹⁰ Vgl. [Teil 4 B. I. 3. e. ee\) \(2\)](#).

¹⁹¹ Ein solches Misstrauen wäre eine Kontrollbarriere, vgl. [Teil 1 A. III. 11](#).

¹⁹² Vgl. [Teil 3 C. XI](#).

¹⁹³ Bezogen auf alle Kontrolleure auch *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 14.

aa) Rechtliche Kontrollbarrieren

Dem BfDI können Kontrollen mit Hinweis auf eine Verletzung der Third-Party-Rule bzw. des Staatswohls verweigert werden¹⁹⁴. Die Ermächtigung des Bundesinnenministeriums gem. § 28 Abs. 3 S. 3 BVerfSchG (bzw. des Bundeskanzleramts und des Verteidigungsministeriums gem. § 62 BNDG i. V. m. § 28 Abs. 3 S. 3 BVerfSchG und § 13a MADG i. V. m. § 28 Abs. 3 S. 3 BVerfSchG), einzelne Kontrollmittel mit Verweis auf das Staatswohl zu verweigern, muss gestrichen werden.¹⁹⁵

Grundsätzlich ist es nicht überzeugend, dass der BND den Third Party-Vorbehalt gegenüber dem UKRat nicht geltend machen kann, gegenüber dem BfDI jedoch schon. Auch der BfDI ist – wie der UKRat – ein unabhängiges Organ innerhalb der Exekutive¹⁹⁶. Da der UKRat nicht als „Dritter“ wahrgenommen wird, sollte dies für den BfDI logischerweise auch gelten. Letztlich widersprechen die Ausnahmetatbestände der Logik des Kontrolldesigns: Weil Betroffene aus Geheimschutzgründen selbst faktisch so gut wie keine Möglichkeiten haben, sich zu wehren, sollen unabhängige Kontrolleure diese Aufgabe übernehmen, um so zur Verhältnismäßigkeit der eingriffsintensiven Maßnahmen beizutragen. Verweigert man allerdings den unabhängigen Rechtskontrolleuren die Kontrollmöglichkeit, sind diese Datenverarbeitungen unverhältnismäßig. Weil die Verhältnismäßigkeit aber notwendige Voraussetzung für die rechtsstaatliche Legitimität nachrichtendienstlicher Tätigkeit ist, liegt es sogar im Interesse der Nachrichtendienste, gegenüber den unabhängigen Kontrolleuren keine Kontrollbarrieren zu errichten.

Um berechtigten Geheimhaltungsbedenken der Aufsichtsbehörden und Nachrichtendienste dennoch Rechnung zu tragen, sind vielfältige Schutzmechanismen denkbar, unter anderem eine bessere räumliche Abschirmung der Kontrolleure, verschärfte Standards bei den Sicherheitsüberprüfungen und ausgebaute Sanktionsregime bei Verstößen gegen Verschwiegenheitspflichten.

¹⁹⁴ Vgl. Teil 3 D. II. 7. b.

¹⁹⁵ So bereits *Schwabenbauer*, Heimliche Grundrechtseingriffe, S. 354; *Gusy*, Richterliche Kontrolle, 67, 90.

¹⁹⁶ Vgl. [Teil 1 A. I. 1. b.](#)

bb) Ressourcenbarrieren

Es muss regelmäßig geprüft werden, ob der BfDI über eine ausreichende Stellenanzahl zur Kontrolle der Nachrichtendienste verfügt. Falls den Nachrichtendiensten neue Befugnisse verliehen werden oder diese einen erheblichen Stellenzuwachs erfahren, müssen die Kapazitäten des BfDI möglicherweise angepasst werden.¹⁹⁷

5. Umsetzung des Kontrollgesamtüberblicks

Damit ein Kontrolleur potenziell alle Maßnahmen der Nachrichtendienste gegenüber einer Person in den Blick nehmen kann (Kontrollgesamtüberblick), müsste man Folgendes ändern: Erstens sollte der BfDI ein umfassendes Einsichtsrecht haben (a.), zweitens sollte die Kooperation zwischen dem GeKon und dem BfDI verbessert werden (b.).

a. Umfassendes Einsichtsrecht des BfDI

Nach der Rechtsprechung soll mindestens ein Kontrolleur über Zugang zu allen Daten und nicht „nur ein[em] eingeschränkte[n] Datenbestand“ verfügen. Dafür könnte man ihm ein umfassendes Einsichtsrecht in die Datenverarbeitung des Nachrichtendienstes verleihen¹⁹⁸.

Bereits de lege lata verfügt der BfDI über einen potenziell sehr weitgehenden Überblick über alle Datenverarbeitungen¹⁹⁹. Als Folge der vorgeschlagenen Auflösung der G 10-Kommission entfällt ihre singuläre Zuständigkeit für die Kontrolle von Eingriffen in Art. 10 GG. Diese Aufgabe wird dann vom BfDI wahrgenommen. Dies führt in Verbindung mit der Streichung der Ausnahmetatbestände dazu, dass der BfDI die Möglichkeit hat, sich einen Kontrollgesamtüberblick zu verschaffen.

b. Verstärkte Kooperation zwischen den Aufsichtsbehörden

Zusätzlich müsste die Zusammenarbeit zwischen den Kontrolleuren verbessert werden. Die vielfach kritisierte²⁰⁰ Begrenzung der Austauschmöglichkeiten auf die Erörterung „allgemeiner Angelegenheiten“ (§ 58 Abs. 3 BNDG) sollte aufgehoben werden, sodass die Kontrolleure sich zu konkreten Fällen beraten können. Nebenbei würde man auf

¹⁹⁷ Darauf hinweisend beispielsweise *Bergemann*, NVwZ 2015, 1705, 1709; bezüglich des UKRats *Wetzling*, Bedingt kontrollfähig, S. 21.

¹⁹⁸ Vgl. [Teil 1 A. III. 5.](#)

¹⁹⁹ Vgl. [Teil 3 F. I.](#)

²⁰⁰ U.a. *BfDI*, Stellungnahme zum Gesetzesentwurf zur Änderung des BNDG, S. 10; darüber hinaus schlägt *Wetzling* weitere Zusammenarbeitsmöglichkeiten vor, *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15.

diese Weise den Aufwand der Nachrichtendienste, der durch „unkoordiniert[e] Kontrollersuchen“ entsteht, verringern.²⁰¹ Ein solcher Austausch muss in der Praxis dann auch stattfinden²⁰². Um das sicherzustellen, könnte man eine Kooperationspflicht statuieren. Denkbar wäre beispielsweise, dass Kontrolleure auf Anfragen eines anderen Kontrolleurs zeitnah reagieren müssen und zu inhaltlichem Austausch verpflichtet werden. Es wäre zudem sinnvoll, dass Kontrollbesuche²⁰³ bei den Nachrichtendiensten gemeinsam erfolgen. Damit würde man zum einen die Ressourcen der Nachrichtendienste schonen, zum anderen verfügten die Kontrolleure stets über dieselben Informationen.

6. Der BfDI als internationaler Ansprechpartner

Die Arbeit der Nachrichtendienste des Bundes besteht zu erheblichen Teilen aus Kooperationen mit ausländischen Nachrichtendiensten und zum Teil mit supranationalen Institutionen, wie beispielsweise der NATO, EU-Intcen²⁰⁴ und Counter Terrorist Group²⁰⁵ als Mechanismen der Europäischen Union. Diese Zusammenarbeit muss kontrolliert werden.²⁰⁶

De lege lata kann der BfDI auch Datenübermittlungen ins Ausland kontrollieren, allerdings hat er gegenüber ausländischen Behörden keine Kontrollbefugnis mehr. Übermittlungen werden häufig mit einschränkenden Vorgaben zur Nutzung der Daten verbunden, weshalb der zuständige Kontrolleur „jenseits der Grenze“ die Kontrolle weiterführen müsste. Bisher gibt es keine Regelungen für die grenzüberschreitende Kooperation der Kontrolleure²⁰⁷:

²⁰¹ Gärditz, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 14.

²⁰² Sosna, GSZ 2022, 245, 251.

²⁰³ Diesen Aspekt betont Wetzling im Zusammenhang mit Kooperationen zwischen der G 10-Kommission und dem BfDI, Wetzling, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 15.

²⁰⁴ Conrad, European Foreign Affairs Review 2021, 55; [European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs](#) (2013/2188(INI)), S. 23.

²⁰⁵ Conrad, European Foreign Affairs Review 2021, 55; Monroy, Geheimdienste auf Abwegen.

²⁰⁶ [European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs](#) (2013/2188(INI)), S. 23 Rn. 77; trotzdem erfolgt jedenfalls ein allgemeiner Austausch zu Best Practice-Modellen im [European Intelligence Oversight Network \(EION\)](#).

²⁰⁷ Sosna, GSZ 2022, 245, 248.

“Moreover, existing control mechanisms (...) are nationally limited, as each State looks exclusively at its own agencies, and none looks at the international network of cooperation as a whole.”²⁰⁸

Die Lösung dieser aus rechtsstaatlicher Perspektive problematischen Situation ist in dieser Untersuchung nicht beabsichtigt. Wenn aber ein Kooperationsregime der Kontrolleure geschaffen würde, wäre der BfDI – unter Beachtung der hier vorgestellten Anpassungen seiner normativen Grundlagen – aufgrund seines Kontrollgesamtüberblicks prädestiniert dafür, die Rolle des deutschen Ansprechpartners zu übernehmen.²⁰⁹

Für die Vorabkontrolle stellt sich das Problem nicht, weil die Genehmigung nur durch einen Kontrolleur erteilt werden kann.

7. Evaluierung von Kontrolllücken

Die Kontrolleure müssen die Parlamente, mindestens aber die Parlamentarischen Kontrollgremien, in angemessenen Abständen darüber informieren, inwieweit sie Kontrolllücken identifiziert haben. Denn in Folge der Digitalisierung und Automatisierung ist mit ständigen Veränderungen in der nachrichtendienstlichen Praxis zu rechnen, wodurch Änderungen im Kontrolldesign laufend erforderlich sind.²¹⁰

Deshalb wird vorgeschlagen, die Berichtspflichten der Kontrolleure gegenüber dem PKGr auf diesen Aspekt zu erstrecken.

8. Zwischenergebnis

Auf der Bundesebene soll es nach diesem Vorschlag künftig zwei für die externe Rechtskontrolle zuständige Institutionen geben: erstens das GeKon als Vorabkontrolleur für alle eingriffsintensiven Maßnahmen der Nachrichtendienste des Bundes; zweitens den BfDI als Datenschutzkontrolleur für alle Datenverarbeitungen der Nachrichtendienste des Bundes. Dabei kann auf vorhandene Normen zurückgegriffen werden, die jedoch in vielerlei Hinsicht überarbeitet werden müssen. Im Ergebnis würden wichtige Probleme der Rechtskontrolle auf der Bundesebene behoben, weil die Voraussetzungen für durchschaubarere Kontrollstrukturen geschaffen werden, die Anzahl der Kontrolleure verringert wird und ein potenzieller Gesamtüberblick entsteht.

²⁰⁸ Venedig-Kommission, Report 2015, S. 14 Rn. 67.

²⁰⁹ Wetzling fordert in Bezug auf den UKRat, dass dieser eine „Vollmitgliedschaft in der European Working Group on Intelligence Oversight“ beantragen solle, Wetzling, Bedingt kontrollfähig, S. 21.

²¹⁰ BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17 - Rn. 299; Wetzling/Vieth, Datenbasierte Nachrichtendienstkontrolle, S. 57 f.

II. Reform der externen Rechtskontrolle auf der Landesebene

Viele auf der Bundesebene relevante Aspekte gelten für die Reform der externen Rechtskontrolle der Nachrichtendienste in den Ländern gleichermaßen. Allerdings gibt es – vor allem auf Grund geringer Ressourcen – auf der Landesebene mehr Änderungsbedarf als im Bund.

1. Auflösung der G 10-Kommissionen

Wie auf der Bundesebene wird auch für die Länder die Auflösung der G 10-Kommissionen vorgeschlagen.²¹¹ Da die G 10-Kommissionen in den Landesverfassungen nicht erwähnt werden, sind dafür keine Verfassungsänderungen erforderlich.²¹² Allerdings ist die Auflösung der G 10-Kommissionen nur möglich, wenn § 16 G 10 dahingehend angepasst wird, dass eine „parlamentarische“ Kontrolle auf der Landesebene zukünftig nicht mehr erforderlich ist.

Für die Genehmigung eingriffsintensiver Maßnahmen sollten stattdessen Richter zuständig sein.

Unbedingt vermieden werden muss eine Regelungsweise, bei der die unabhängige Vorabkontrolle zwar größtenteils einem Gericht übertragen wird, die G 10-Kommission aber für Genehmigungen zuständig bliebe. Denn damit würde die Chance vertan, die dysfunktional hohe Anzahl an Kontrolleuren²¹³ zu reduzieren. Im Gegenteil entstünden unterschiedliche Kontrollniveaus: so ist das Gericht hauptamtlich tätig, die G 10-Kommission nur nebenamtlich. Wegen des Richtervorbehalts bei Wohnraumüberwachungen gab es diese Zweiteilung zwar auch bisher, allerdings hat die Wohnraumüberwachung kaum praktische Bedeutung in der nachrichtendienstlichen Tätigkeit, wodurch sich das unterschiedliche Kontrollniveau bisher kaum ausgewirkt hat. Wenn die Vorabkontrolle hingegen auf weitere, praxisrelevantere Befugnisse ausgeweitet wird, wirken sich die unterschiedlichen Kontrollniveaus zwangsläufig stärker aus.

²¹¹ Sollte es keine politische Bereitschaft geben, die G 10-Kommissionen aufzulösen, müssen zumindest die vielfältigen verfassungsrechtlichen Mängel behoben werden (vgl. insoweit ab Teil 3 B. II. 1. b., vgl. insoweit auch *Gusy*, VerwArch 2015, 437, 449: „Die ehrenamtliche Tätigkeit der Mitglieder, die insbesondere in den Ländern nicht stets zureichende Ausstattung der Kommission und deren partiell defizitäres Bewusstsein um den eigenen Kontrollauftrag nach Abschluss der Überwachungsmaßnahme selbst – also der Informationsverwendung – zeigen Schwachstellen, die beseitigt werden müssen.“

²¹² [Art. 16 Abs. 2 der LV Bbg](#) legt fest, dass mindestens eine „nachträgliche richterliche Kontrolle“ erfolgen muss; [Art. 27 Abs. 2 S. 2 der SächsLV](#) entspricht Art. 10 Abs. 2 S. 2 GG.

²¹³ Vgl. [Teil 4 A. I.](#)

Mit Rücksicht auf die bedeutende Tätigkeit der Nachrichtendienste muss unbedingt verhindert werden, dass wegen politischen Postenverteilungslogiken ein Kontrollorgan wie die G 10-Kommission erhalten bleibt, für dessen Weiterbestehen sachliche Gründe nicht ersichtlich sind.

Die Datenschutzkontrolle von Eingriffen in Art. 10 GG soll von den Landesdatenschutzbeauftragten wahrgenommen werden.

2. Vorabkontrolle durch ein Landes-GeKon?

Auf der Landesebene gibt es keine dem UKRat vergleichbaren Institutionen. In einzelnen Bundesländern ein Pendant zum UKRat zu errichten, wäre zwar möglich, wegen des erheblichen finanziellen Aufwands allerdings zumindest für kleinere Bundesländer kaum realisierbar²¹⁴ und in Anbetracht der teilweise geringen Mitarbeiteranzahl des zu kontrollierenden Nachrichtendienstes nicht notwendig.

Denkbar wäre jedoch, auf der Landesebene eine dem GeKon vergleichbare Institution zu schaffen und diese über eine staatsvertragliche Vereinbarung in allen Ländern einzubeziehen. Mit der Kinder- und Jugendmedienanstalt (KJM) als „Wanderorgan“ der Landesmedienanstalten gibt es ein regulatorisches Vorbild, an dem die Gesetzgeber sich orientieren können. Die KJM wurde geschaffen, um die „Zersplitterung der Aufsichtsstrukturen beim Jugendschutz“ zu überwinden.²¹⁵ Sie ist länderübergreifend für die Aufsicht von Rundfunk und Telemedien zuständig, ist aber selbst keine Behörde, sondern wird als Organ der jeweils zuständigen Landesmedienanstalt tätig.²¹⁶

Nach der Rechtsprechung des Bundesverfassungsgerichts muss die Gebietskörperschaft, der das Grundgesetz gem. Art. 83 ff. GG eine Verwaltungskompetenz überträgt, diese Aufgabe durch ihre eigene Verwaltung wahrnehmen; hiervon kann in eng umgrenzten Materien jedoch eine Ausnahme zugelassen werden.²¹⁷ Da die Bundesländer für den Landesverfassungsschutz zuständig sind und die Kontrollstruktur daran anknüpft²¹⁸, muss die Kontrolle grundsätzlich durch eine Institution des jeweiligen Bundeslands erfolgen. Bei der Vorabkontrolle der Verfassungsschutzbehörden handelt es sich – wie beim Jugendmedienschutz – allerdings um eine eng begrenzte Materie, für die eine Ausnahme von diesem Grundsatz denkbar wäre.

²¹⁴ Michel, Verfassungsblog vom 18.7.2022; Gärditz, Verfassungsblog vom 2.5.2022; vgl. auch „Anlage 3: Institutionelle Anforderungen an unabhängige Kontrollen“ der Bund-Länder-AG zu BVerfGE v. 26.4.2022 zum BayVSG, S. 9, https://www.imk2022.bayern.de/wp-content/uploads/2022/09/22-06-21-Abschlussbericht-der-Bund-La%CC%88nder-AG_BVerfG-zu-BayVSG.pdf (abgerufen am 31.8.2024).

²¹⁵ Liesching, § 14 JMStV Vorbem.

²¹⁶ Binder/Vesting/Schulz/Dreyer, § 14 JMStV Rn. 1 f.

²¹⁷ Binder/Vesting/Schulz/Dreyer, § 14 JMStV Rn. 10; BVerfG, Beschluss v. 12.1.2013 - 2 BvL 23/81 - Rn. 131.

²¹⁸ Vgl. Teil 1 B. I. 2.

Dabei ist jedoch zu beachten, dass Verwaltungskompetenzen nicht auf einen anderen Kompetenzträger übertragen werden dürfen, weshalb die KJM als Organ der zuständigen Landesmedienanstalt tätig wird.²¹⁹ Das bedeutet, dass es in jedem Bundesland einen zuständigen Kontrolleur geben muss, für den das Landes-GeKon tätig wird. Denkbar wäre, jeweils eine eigene Vorabkontrollinstitution mit wenigen Mitarbeitern zu etablieren. Alternativ könnte das Landes-GeKon für die G 10-Kommissionen der Länder tätig werden.

Darüber hinaus muss verhindert werden, dass ein Kompetenzträger die Willensbildung der Behörde eines anderen „wesentlich“ beeinflusst.²²⁰ Es muss also darauf geachtet werden, dass nicht allein ein Land über die Besetzung des Landes-GeKon entscheidet, zumindest soweit es als Vorabkontrollleur für andere Landesverfassungsschutzbehörden agiert.

Zudem muss es sachliche Gründe für die Kooperation mit einem anderen Kompetenzträger geben.²²¹ Die Einbeziehung anderer Länder in die Vorabkontrolle der eingriffsintensiven Maßnahmen von Landesverfassungsschutzbehörden ist sinnvoll, weil eine professionelle Kontrolle in kleinen Bundesländern nur schwer umsetzbar ist. Außerdem könnte so für die Vorabkontrolle ein bundeseinheitlicher Standard garantiert werden. Darüber hinaus würde der Zersplitterung der Kontrolleure entgegengewirkt.

Der Nachteil dieser Lösung ist, dass sie mit einem hohen Aufwand verbunden ist und einen länderübergreifenden, gesetzgeberischen Gestaltungs- und Kooperationswillen voraussetzt, der sich bisher nicht abzeichnet.²²²

3. Vorabkontrolle durch Richter

Eine vergleichsweise leicht umsetzbare Lösung besteht darin, bei der Vorabkontrolle auf die Landesgerichtsbarkeit zurückzugreifen.²²³ Die Einführung eines Richtervorbehalts hat auf der Landesebene einige Vorteile (vgl. a.). Da mit der Novellierung der Verfassungsschutzgesetze in Bayern und Hessen das Urteil zum bayerischen Verfassungsschutzgesetz vergleichsweise schnell umgesetzt wurde, werden sie eine Vorbildfunktion

²¹⁹ Binder/Vesting/Schulz/Dreyer, § 14 JMStV Rn. 11; Spindler/Schuster/Erdemir, § 14 JMStV Rn. 14.

²²⁰ Binder/Vesting/Schulz/Dreyer, § 14 JMStV Rn. 12.

²²¹ Binder/Vesting/Schulz/Dreyer, § 14 JMStV Rn. 12; BVerfG, Beschluss v. 12.1.2983 - 2 BvL 23/81 - Rn. 131.

²²² Anders als die KJM müsste das GeKon außerdem 16 unterschiedliche Verfassungsschutzgesetze prüfen, weil es keine einheitliche Rechtsgrundlage gibt.

²²³ „Am einfachsten dürften sich diese in Form von Richtervorbehalten implementieren lassen. Dieser Ansatz hat den Vorteil, dass man auf vorhandene bewährte Strukturen zurückgreifen könnte.“, Bantlin/Graulich, GSZ 2023, 179, 182.

für andere Landesgesetzgeber entfalten. Ihre Regelungsweise der richterlichen Vorabkontrolle wird daher zunächst kritisch erörtert (b., c.), bevor ausgeführt wird, was beim Kontrolldesign auf der Landesebene generell zu beachten ist (d.).

a. Vorteile der gerichtlichen Vorabkontrolle auf der Landesebene

Sowohl das neue bayerische als auch das hessische und sächsische Landesverfassungsschutzgesetz sehen eine richterliche Vorabkontrolle eingriffsintensiver Maßnahmen vor. Der hessische Gesetzgeber gibt als Begründung seiner Entscheidung für die Kontrolle durch Gerichte und gegen eine Kontrolle durch die jeweiligen G 10-Kommissionen die schnelle Erreichbarkeit in Eilfällen an. Durch den – beim für die Anordnung der Wohnraumüberwachung zuständigen Amtsgericht – „bereits eingerichteten Ermittlungsrichtereildienst und Bereitschaftsdienst“ werde „die Erreichbarkeit in Eilfällen in größtmöglichem Umfang gewährleistet“. So ließen sich Eilanordnungen durch das LfV „auf ein Minimum“ reduzieren.²²⁴

In den Gesetzgebungsmaterialien zur bayerischen Reform wird die Entscheidung für gerichtliche Vorabkontrollen und gegen eine Übertragung an die G 10-Kommission nicht begründet.

Dafür, die unabhängige Vorabkontrolle auf der Landesebene Gerichten zu übertragen, spricht zunächst, dass das Bundesverfassungsgericht in seiner Rechtsprechung ohnehin eine Präferenz für gerichtliche Kontrollen geäußert hat und dass die Möglichkeit einer sonst unabhängigen, richterähnlichen Vorabkontrolle eher als Entgegenkommen gegenüber der Exekutive zu interpretieren ist, deren Geheimhaltungsbedenken das Bundesverfassungsgericht gerecht werden wollte.²²⁵ Die Geheimhaltungsbedenken gegenüber einer gerichtlichen Kontrolle können jedoch bei entsprechenden Schutzvorkehrungen entkräftigt werden.²²⁶

Außerdem hat die Beauftragung eines Gerichts den Vorteil, dass damit im Vergleich zu den anderen Optionen der Aufwand am geringsten bleibt, weil auf „bewährte Strukturen“ zurückgegriffen werden kann²²⁷. Im Gegensatz dazu müssten die mit ehrenamtlich tätigen Mitgliedern besetzten G 10-Kommissionen „professionalisiert“²²⁸ und die erheblichen Regelungsdefizite – gerade auf der Landesebene²²⁹ – erst behoben werden.

²²⁴ Drs. 20/10821 v. 21.3.2023, S. 21, <https://starweb.hessen.de/cache/DRS/20/1/10821.pdf>, (abgerufen am 31.8.2024).

²²⁵ Vgl. [Teil 2 A. III. 6. a.](#)

²²⁶ Vgl. [Teil 4 B. II. 3. d. cc.](#)

²²⁷ Bantlin/Graulich, GSZ 2023, 179, 182.

²²⁸ Hipp, Interview mit Matthias Bäcker.

²²⁹ Vgl. [Teil 3 B.](#)

b. Neuregelung des Bayerischen Verfassungsschutzgesetzes

Das Bundesverfassungsgericht hat in seinem Urteil zum Bayerischen Verfassungsschutzgesetz angeordnet, dass die mit dem Grundgesetz nicht zu vereinbarenden Normen in modifizierter Form bis zum Ablauf des 31. Juli 2023 vorübergehend fortgelten können.²³⁰ Daher musste bis zum 1. August 2023 eine Neuregelung in Kraft getreten sein. Bereits im Dezember 2022 hat die Landesregierung einen Gesetzesentwurf für eine Neufassung des bayerischen Verfassungsschutzgesetzes veröffentlicht.²³¹ Die Änderung des Verfassungsschutzgesetzes wurde am 24.7.2023 verkündet.²³²

aa) Befugnisse mit Richtervorbehalt

Der bereits nach dem alten Gesetz vorgesehene Richtervorbehalt für die Online-Durchsuchung und die Wohnraumüberwachung bleibt bestehen (Art. 11 Abs. 1 i. V. m. Art. 9, 10 BayVSG). Darüber hinaus wird eine richterliche Anordnung für bestimmte Formen des Einsatzes Verdeckter Mitarbeiter und Vertrauensleute sowie für längerfristige Observationen vorgeschrieben. Art. 12 BayVSG, der den Einsatz technischer Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes oder zur Ermittlung der Geräte- oder Kartennummer ermöglicht, wurde so umformuliert, dass die Bewegung eines Mobiltelefons oder einer beobachteten Person nur noch „punktuell“ nachverfolgt werden kann. Durch die engere Ausgestaltung handele es sich nur noch um einen Eingriff von „eher geringem Gewicht“.²³³

Eine richterliche Vorabkontrolle sei daher nicht notwendig.

(1) Verdeckte Mitarbeiter (Art. 18 BayVSG)

Die novellierte Rechtsgrundlage zum Einsatz Verdeckter Mitarbeiter unterscheidet zwischen zwei Einsatzmodalitäten. Nach der ersten Alternative (Art. 18 Abs. 1 S. 1

²³⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 403 f.

²³¹ LT-Drs. 18/21537 v. 2.3.2022 https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024).

²³² Bayerisches Gesetz- und Verordnungsblatt Nr. 14/2023 v. 24.7.2023, S. 374, https://www.bayern.landtag.de/www/ElanTextAblage_WP18/GVBl/2023/GVBl-2023-Nr-14.pdf (abgerufen am 31.8.2024).

²³³ LT-Drs. 18/21537 v. 2.3.2022 https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024), S. 38.

BayVSG) ist das Landesamt berechtigt, eigene Mitarbeiter unter einer ihnen verliehenen und auf Dauer angelegten Legende einzusetzen. Die zweite Variante gem. Art. 18 Abs. 1 S. 2 BayVSG legt fest, dass eine Maßnahme mit verdeckten Mitarbeitern, die entweder länger als sechs Monate dauert (Nr. 1), gezielt gegen eine Person (Nr. 2) oder in zu privaten Wohnzwecken genutzten Räumlichkeiten (Nr. 3) eingesetzt wird, nur zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit²³⁴ zulässig sein soll. Bei der ersten Variante muss der Einsatz Verdeckter Mitarbeiter von der Behördenleitung bzw. ihrer Stellvertretung angeordnet werden, eine Genehmigung durch eine externe Stelle ist nicht vorgesehen (Art. 18 Abs. 4 Nr. 1 BayVSG). Demgegenüber ist für den Einsatz eines verdeckten Mitarbeiters unter den Voraussetzungen von Art. 18 Abs. 1 S. 2 BayVSG eine richterliche Genehmigung erforderlich, die nach einem Jahr erneuert werden muss, falls die Maßnahme so lange andauert (Art. 18 Abs. 4 Nr. 2 BayVSG). Begründet wird die unterschiedliche Ausgestaltung damit, dass der kurzzeitige Einsatz von geringerer Eingriffsintensität sei, während die zweite Variante wegen ihrer Dauer oder Intensität ein erhöhtes Eingriffsgewicht aufweise.²³⁵

(2) Vertrauensleute (Art. 19 BayVSG)

Art. 19 Abs. 1 S. 1 BayVSG verweist auf die entsprechende Anwendbarkeit von Art. 18 Abs. 1-4 BayVSG. Eine richterliche Genehmigung ist erst ab einem Einsatz von mehr als sechs Monaten Dauer einzuholen (Art. 19 Abs. 1 S. 2 BayVSG), für kürzere Einsätze oder die Anwerbungsphase ist eine interne Anordnung durch den Behördenleiter bzw. dessen Vertretung vorgesehen. Dass eine genehmigungsfreie Anwerbungsphase besteht, wird damit begründet, dass das Bundesverfassungsgericht dies als verfassungskonform erachtet hat, wenn die Phase „von begrenzter Dauer“ ist.²³⁶

(3) Längerfristige Observationen (Art. 19a BayVSG)

Auch die Rechtsgrundlage für längerfristige Observationen unterscheidet zukünftig mehrere Varianten.

²³⁴ Definiert in Art. 4 Abs. 2 Nr. 2 BayVSG.

²³⁵ LT-Drs. 18/21537 v. 2.3.2022, S. 41, https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/%C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024).

²³⁶ LT-Drs. 18/21537 v. 2.3.2022 https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/%C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024), S. 42; BVerfG, Urteil v. 26.4.2022, 1 BvR 1619/17 Rn. 353 f.

Für die als wenig intensiv erachtete²³⁷ Observation gem. Art. 19a Abs. 1 S. 1 BayVSG gilt kein Richtervorbehalt. Sie erfolgt außerhalb der Wohnung durchgehend länger als 48 Stunden oder an mehr als drei Tagen innerhalb einer Woche verdeckt auch mit technischen Mitteln und wird durch den Behördenleiter oder dessen Vertretung angeordnet (Art. 19a Abs. 2 S. 1 Nr. 1 BayVSG).

Demgegenüber gilt für längerfristige Observationen gem. § 19a Abs. 1 S. 2, 3 BayVSG ein Richtervorbehalt²³⁸. Dabei handelt es sich um Observationen, die entweder an nicht öffentlich zugänglichen Orten (S. 2 Nr. 1) oder unter verdecktem Einsatz technischer Mittel zur Herstellung von Lichtbilderfolgen, Ton- und Bildaufzeichnungen oder zur Nachverfolgung der Bewegung im Raum (S. 2 Nr. 2) erfolgen bzw. die durchgehend länger als eine Woche andauern oder an mehr als 14 Tagen eines Monats stattfinden (S. 3 Nr. 1) oder bei denen außerhalb der Öffentlichkeit technische Mittel eingesetzt werden (S. 3 Nr. 2).

(4) Komplexe qualifizierende Anforderungen für den Richtervorbehalt

Dass der Richtervorbehalt beim Einsatz Verdeckter Ermittler nicht generell, sondern nur bei bestimmten, die Eingriffsintensität steigernden Umständen normiert wird, ist verfassungsrechtlich grundsätzlich unbedenklich, da „bei einem nicht nur kurzzeitigen Einsatz, der den Aufbau einer Vertrauensbeziehung noch nicht erwarten lässt“, keine unabhängige Vorabkontrolle erforderlich ist²³⁹. Ob die Tätigkeit Verdeckter Ermittler erst ab einem Zeitraum von über sechs Monaten nicht mehr „kurzzeitig“ ist (Art. 18 Abs. 1 S. 2 Nr. 1 BayVSG) oder man die Grenze bereits zu einem früheren Zeitpunkt ziehen müsste, ist fraglich. Grundsätzlich hat der Gesetzgeber einen Beurteilungsspielraum. Hier ist zu beachten, dass das Bundesverfassungsgericht für den Einsatz von Vertrauensleuten eine genehmigungsfreie Anwerbungs- und Erprobungsphase von begrenzter Dauer anerkannt hat, weil bei unbekannten Vertrauensleuten im Vergleich zu den Verdeckten Ermittlern ein längerer Vorlauf erforderlich sein kann.²⁴⁰ Der Einsatz von Vertrauensleuten ist nach dieser Konzeption wegen seiner Unberechenbarkeit gegenüber dem Einsatz Verdeckter Mitarbeiter insoweit privilegiert, als die Vorabkontrolle auf einen späteren Zeitpunkt verschoben werden kann. Wenn der bayerische Ge-

²³⁷ LT-Drs. 18/21537 v. 2.3.2022 https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024), S. 43.

²³⁸ Art. 19a Abs. 2 S. 1 Nr. 2 BayVSG.

²³⁹ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 Rn. 348.

²⁴⁰ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 Rn. 353.

setzgeber bei beiden Rechtsgrundlagen erst ab einem Einsatz von mehr als sechs Monaten eine unabhängige Vorabkontrolle fordert (Art. 19 Abs. 1 S. 2 BayVSG), wird die in der Rechtsprechung angelegte Privilegierung der Vertrauensleute aufgelöst.²⁴¹ Außerdem ist nicht ersichtlich, wieso die Eingriffsintensität der Maßnahme davon abhängig sein soll, dass der Verdeckte Ermittler seit vier Monaten und nicht seit mehr als sechs Monaten tätig ist. Auch nach vier Monaten kann sich bereits eine Vertrauensbeziehung entwickelt haben. Gerade weil es sich um beliebig ausgewählte Zeiträume handelt, die dem Einzelfall nicht gerecht werden können, wäre es überzeugender, den Einsatz Verdeckter Ermittler generell gerichtlich genehmigen zu lassen. Praktikabler wäre eine solche Regelung ohnehin, da die aufwändige Prüfung der Voraussetzungen von Art. 18 Abs. 1 S. 2 BayVSG entfallen würde.

Ein ähnliches Problem stellt sich bei Art. 19a BayVSG. Der Gesetzgeber möchte nicht-langfristige Observationen im Einklang mit den Ausführungen des Bundesverfassungsgerichts²⁴² gegenüber langfristigeren und kernbereichsensibleren Observationen insoweit privilegieren, als eine externe Genehmigung nicht eingeholt werden muss (Art. 19a Abs. 1 S. 1, Abs. 2 Nr. 1 BayVSG). Eine nicht-langfristige Observation dauert gem. Art. 19 Abs. 1 S. 3 Nr. 1 BayVSG nicht „durchgehend länger als eine Woche“ oder findet nicht „an mehr als 14 Tagen eines Monats“ statt. Ob der Begriff der „längerfristigen“ Observation damit verfassungskonform ausdifferenziert wurde, ist sehr fragwürdig. Dagegen spricht, dass das Bundesverfassungsgericht die Observation gem. Art. 19a Abs. 1 S. 1 BayVSG, die durchgehend länger als 48 Stunden oder an mehr als drei Tagen innerhalb einer Woche erfolgt, als langfristig eingeordnet hat.²⁴³ In dieser Randnummer verweist das Gericht auf die Entscheidung zum Bundeskriminalamtsgesetz²⁴⁴, in der es unter anderem die Verfassungsmäßigkeit einer längerfristigen Observation (§ 20g Abs. 2 Nr. 1 BKAG a.F.) zu beurteilen hatte. Nach dieser Norm ist eine langfristige Observation bereits zu bejahen, wenn sie „durchgehend länger als 24 Stunden dauern oder an mehr als zwei Tagen stattfinden soll“.²⁴⁵ Zwar hat der Gesetzgeber bei der Auslegung des Begriffs „längerfristig“ einen Beurteilungsspielraum. Dennoch spricht vieles dafür, dass die Zeitspanne, in der noch keine externe Genehmigung einzuholen ist, hier zu lange bemessen ist.

²⁴¹ Deshalb die genehmigungsfreie Anwerbungsphase für Vertrauenspersonen zu verlängern, kommt nicht in Betracht, weil es dann vermutlich kein Zeitraum „von begrenzter Dauer“ mehr wäre, vgl. BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 353.

²⁴² BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 361.

²⁴³ „Die durch Art. 19a BayVSG erlaubten langfristigen Observationen (...)“, BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 357.

²⁴⁴ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 176.

²⁴⁵ Vgl. insoweit auch die Definitionen in § 14 Abs. 1 S. 1 Nr. 7 [NVerfSchG](#); § 8 Abs. 2 S. 3 Nr. 3 [LVerfSchG SH](#).

bb) Ausgestaltung der richterlichen Kontrolle

In den neu geschaffenen Artt. 29 ff. BayVSG wird die in den oben beschriebenen Rechtsgrundlagen etablierte richterliche Vorabkontrolle detailliert. Zuständig ist das Amtsgericht am Sitz des Landesamtes, bei Beschwerden das Oberlandesgericht (Art. 29 BayVSG, § 120 Abs. 4 S. 2 GVG). Für das gerichtliche Verfahren gilt das erste Buch des FamFG entsprechend, mit der Besonderheit, dass Betroffene nicht angehört und ihnen Entscheidungen nicht mitgeteilt werden dürfen (Art. 30 Abs. 1 BayVSG). Eine Anfechtungsklage gegen richterliche Entscheidungen ist ausgeschlossen (Art. 30 Abs. 2 BayVSG). Gem. Art. 30 Abs. 3 BayVSG dürfen die Entscheidungen des Gerichts und Unterlagen über Maßnahmen in den Gerichtsakten nicht gespeichert werden, sondern werden beim Landesamt aufbewahrt. Inwieweit der Geheimschutz bei Gericht sichergestellt werden soll, ergibt sich aus diesen Normen nicht. In der Gesetzesbegründung wird darauf hingewiesen, dass die richterliche Vorabkontrolle „eine mit entsprechenden Sachaufwänden verbundene besondere technische und räumliche Ausstattung der Gerichte“ und eine erweiterte Sicherheitsüberprüfung des Personals der Geschäftsstelle bei Gericht voraussetze.²⁴⁶

Das LfV ist gem. Art. 30 Abs. 1 S. 3 BayVSG i. V. m. § 96 StPO analog zur Vorlage von Urkunden und Akten sowie zur Übermittlung elektronischer Dokumente oder zu Auskünften nicht verpflichtet, wenn „das Bekanntwerden des Inhalts dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen“. Im Gegensatz dazu darf die G 10-Kommission Einsicht in alle Dokumente nehmen (vgl. Art. 2 [AGG10BY](#)²⁴⁷). Mit Verweis auf eine Gefährdung des Staatswohls darf ihr die Akteneinsicht nicht verwehrt werden.²⁴⁸ Diese Privilegierung der G 10-Vorabkontrollen gegenüber der richterlichen Kontrolle anderer eingriffsintensiver Maßnahmen ist aus verfassungsrechtlicher Perspektive nicht nachvollziehbar. Aus der Verfassungsrechtsprechung ergibt sich, dass der Vorabkontrolleur über den Sachstand umfassend zu informieren ist und in der Begründung für nachrichtendienstliche Entscheidungen alle „beurteilungsrelevanten Aspekte“ offenzulegen sind.²⁴⁹ Eine Ausnahme für besonders sensible Informationen ist darin nicht angelegt. Aus der Gesetzesbegründung ergibt sich,

²⁴⁶ LT-Drs. 18/21537 v. 2.3.2022 https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024), S. 18, 41. Die Richter seien gem. Art. 2 Abs. 2 BaySÜG nicht zu überprüfen.

²⁴⁷ Vgl. [Teil 3 B. VIII](#).

²⁴⁸ Schenke/Graulich/Ruthig/Huber, § 15 G 10 Rn. 48.

²⁴⁹ Vgl. [Teil 2 A. III. 1. a. gg](#); BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 215.

dass bei Gericht weitreichende Geheimhaltungsvorkehrungen zu treffen sind.²⁵⁰ Dies spricht dagegen, die Einsichtnahme in bestimmte Akten zu verweigern. Denn da der im Rahmen der Kontrolle vorzunehmende Vergleich zwischen dem Ist- und dem Soll-Zustand voraussetzt, dass der Kontrolleur über den zu kontrollierenden Vorgang informiert ist, muss diesem der Zugang zu zuverlässigen, vollständigen und aktuellen Informationen gewährt werden.²⁵¹

cc) Kernbereichsschutzvorkehrungen

Nach dem novellierten bayerischen Verfassungsschutzgesetz ist das Amtsgericht zugleich „unabhängige Stelle“ zum Schutz des Kernbereichs privater Lebensgestaltung und der Daten von Berufsheimnisträgern.²⁵² Die bisherige Zuständigkeit der G 10-Kommission ist weggefallen.²⁵³

dd) Beibehaltung der G 10-Kommission

Nach dem neuen bayerischen Verfassungsschutz gibt es zwei Stellen, die für die Genehmigung der eingriffsintensiven nachrichtendienstlichen Befugnisse zuständig sind: Das Gericht genehmigt Wohnraumüberwachungen und Online-Durchsuchungen, längerfristige Observationen sowie bestimmte Formen des Einsatzes von menschlichen Quellen (HUMINT) und die G 10-Kommission genehmigt Telekommunikationsüberwachungen gem. § 3 Abs. 1 G 10²⁵⁴.

Angesichts der zerklüfteten Kontrolllandschaft sollten Kontrollinstitutionen aufgelöst werden, wenn sie nicht mehr erforderlich sind. Das gilt vor allem für die G 10-Kommissionen der Länder, wenn die Genehmigung der eingriffsintensiven Befugnisse ansonsten Gerichten übertragen wird. Dann sollten alle eingriffsintensiven Maßnahmen – auch die, für die die G 10-Kommission zuständig war – von Gerichten genehmigt werden. Damit die Auflösung der G 10-Kommissionen kein Bundesrecht verletzt, muss jedoch zunächst § 16 G 10 angepasst werden.²⁵⁵

²⁵⁰ LT-Drs. 18/21537 v. 2.3.2022 https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/%C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024), S. 18.

²⁵¹ Gusy, VerwArch 2015, 437, 443.; Bantlin, G 10-Kommission, S. 92; Kahl, Kontrolle, 459, 545; Waldboff, Kontrolle, 73, 74.

²⁵² Art. 8a Abs. 1 S. 5 BayVSG, vgl. Teil 3 E. I. 3.

²⁵³ LT-Drs. 18/21537 v. 2.3.2022 https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/%C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024), S. 30.

²⁵⁴ Art. 2 Abs. 1 S. 3 AGG10BY; vgl. Teil 3 B. II.

²⁵⁵ Vgl. Teil 4 B. I. 1. c.

c. Neuregelung des Hessischen Verfassungsschutzgesetzes

Auch die hessische Landesregierung hat einen Gesetzesentwurf für eine Neuregelung des Verfassungsschutzgesetzes eingebracht.²⁵⁶ Das Gesetz wurde am 11.8.2023 verkündet.²⁵⁷

aa) Befugnisse mit Richtervorbehalt

Wie in Bayern soll der Einsatz bestimmter nachrichtendienstlicher Mittel auch in Hessen unter den Vorbehalt einer richterlichen Anordnung gestellt werden (§ 5a Abs. 1 HVSG). Der bereits nach dem alten Gesetz vorgesehene Richtervorbehalt für die Wohnraumüberwachung bleibt bestehen (§ 8 Abs. 1 HVSG). Darüber hinaus wurde ein Genehmigungsvorbehalt für den Einsatz von IMSI-Catchern zur Standortermittlung (§ 9 Abs. 1 HVSG), für längerfristige Observationen (§ 11 Abs. 2, 4 HVSG) und für den Einsatz von verdeckten Mitarbeitern und Vertrauensleuten etabliert (§§ 12, 13 Abs. 1 HVSG).

(1) Einsatz von IMSI-Catchern zur Ermittlung eines Standorts (§ 9 Abs. 1 HVSG)

Die Norm zum Einsatz von IMSI-Catchern ist erheblich differenzierter und komplizierter als vor der Reform. Gem. § 9 Abs. 1 HVSG soll künftig zwischen dem Einsatz zur Ermittlung einer Geräte- oder Kartennummer (Nr. 1) und dem Einsatz zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunkgeräts (Nr. 2) unterschieden werden. Soweit der IMSI-Catcher zur Standortermittlung verwendet wird und damit keine „operative Maßnahme“, wie beispielsweise eine Observation, vorbereitet werden soll, sondern es um die Erstellung eines „Bewegungsprofils“ geht und der IMSI-Catcher zu diesem Zweck an mehr als „drei aufeinanderfolgenden Tagen mehrfach täglich eingesetzt werden“ soll, muss eine richterliche Anordnung erfolgen (§ 9 Abs. 2, Abs. 3 S. 2 HVSG).

Mit dieser Regelungstechnik verkennt der hessische Gesetzgeber die hohe Eingriffsintensität seiner Befugnis zum Einsatz von IMSI-Catchern. Es hat den Anschein, dass die komplizierte Ausgestaltung von § 9 HVSG dem Zweck dient, wichtige Einsatzbereiche des IMSI-Catchers von der Genehmigungspflicht zu befreien.

Das ist zwar grundsätzlich verfassungskonform möglich, da die Befugnis zum Einsatz eines IMSI-Catchers nach der Rechtsprechung nicht zwingend mit einem tiefen

²⁵⁶ Drs. 20/8129 v. 22.3.2022 in Form des Änderungsantrags Drs. 20/10821 v. 21.3.2023, <https://starweb.hessen.de/cache/DRS/20/1/10821.pdf> (abgerufen am 31.8.2024).

²⁵⁷ Gesetz- und Verordnungsblatt für das Land Hessen v. 11.8.2023, H 13614, S. 614 ff., <https://starweb.hessen.de/cache/GVBL/2023/00027.pdf> (abgerufen am 31.8.2024).

Grundrechtseingriff verbunden ist. So liegt wegen der „begrenzten Aussagekraft“ der Daten kein schwerer Eingriff vor, wenn die Daten einmalig erhoben werden. Eine Norm, die für den Einsatz des IMSI-Catchers hingegen keine zeitliche Grenze festlegt, erlaubt es, den Standort wiederholt und *länger andauernd* zu ermitteln, wodurch sich ein *Bewegungsprofil* der Person erstellen lässt. Ob ein Bewegungsprofil erstellt werden kann, ist für die rechtliche Bewertung der Eingriffsintensität ausschlaggebend.²⁵⁸ Demgegenüber ist eine solche Maßnahme weniger eingriffsintensiv, wenn sie nur punktuell erfolgt.

Wenn die Maßnahme der „Ermöglichung“ einer anderen Maßnahme dient, führt das – anders als der hessische Gesetzgeber annimmt – nicht zu einer geringeren Eingriffsintensität. Die Eingriffsintensität wird nicht erst dadurch gesteigert, dass die Behörde auf die Erstellung eines Bewegungsprofils abzielt, sondern bereits, weil ihr die Daten zur Verfügung stehen und sie die Möglichkeit zur Erstellung eines Bewegungsprofils hat (und sei es als Nebenfolge der Erhebung zu einem anderen Zweck). Zudem ist die Nutzungsbegrenzung auf nicht mehr als an „drei aufeinanderfolgenden Tagen mehrfach täglich“ zu weit gefasst. Innerhalb dieses Zeitraums kann ebenso ein Bewegungsprofil erstellt werden wie dann, wenn zwischen dem dritten und fünften Tag der Nutzung ein oder mehrere Tage pausiert würde.

Verfassungskonform wäre die Norm, wenn ihr Einsatz nur punktuell ermöglicht würde oder wenn der Einsatz eines IMSI-Catchers stets einer richterlichen Anordnung bedürfte.

(2) Längerfristige Observationen (§ 11 Abs. 2, 4 HVSG)

Längerfristige Observationen gem. § 11 Abs. 2 HVSG, die im Einzelfall länger als 48 Stunden dauern oder an mehr als drei Tagen innerhalb einer Woche erfolgen, sind genehmigungsbedürftig (§ 11 Abs. 4 HSVG).

(3) Verdeckte Mitarbeiterinnen und Mitarbeiter (§ 12 HVSG)

Der Einsatz Verdeckter Mitarbeiter muss gem. § 12 Abs. 3 S. 1 HVSG gerichtlich angeordnet werden. Die Anordnung muss auf maximal zwölf Monate befristet werden und kann um jeweils nicht mehr als zwölf Monate verlängert werden, wenn die Voraussetzungen der Anordnung weiterhin fortbestehen und ihr Einsatz unter Berücksichtigung der Gesamtdauer weiterhin verhältnismäßig ist (§ 12 Abs. 3 S. 3, 4 HVSG).

²⁵⁸ Vgl. [Teil 2 A. III. 4. a. aa\).](#)

(4) Vertrauensleute (§ 13 HVSG)

Auch der Einsatz von Vertrauensleuten ist genehmigungspflichtig, § 13 Abs. 1 i. V. m. § 12 Abs. 3 HVSG.

bb) Ausgestaltung der richterlichen Kontrolle

§ 5a HVSG enthält nähere Angaben zur richterlichen Kontrolle (1). Die Norm ist kritikwürdig, insoweit sie die Vorabkontrolle des Einsatzes von Verdeckten Mitarbeitern und Vertrauensleuten zu sehr beschränkt (2). Zudem fehlt es an Vorgaben für die notwendige Abschirmung des Gerichts (3).

(1) § 5a HVSG

Für die Anordnung zuständig ist das Amtsgericht am Sitz des Landesamts für Verfassungsschutz, das Verfahren richtet sich nach den Vorgaben des FamFG (§ 5a Abs. 1, 2 HVSG). Bei Gefahr in Verzug soll die Anordnung von der Behördenleitung oder ihrem Vertreter getroffen werden können, die richterliche Entscheidung muss unverzüglich nachgeholt werden (§ 5a Abs. 6 HVSG). Darüber hinaus müssen die Anträge an das Gericht substantiiert begründet werden und alle beurteilungsrelevanten Tatsachen beinhalten, insbesondere müssen die Zielpersonen, die ggf. zu überwachenden Räume sowie Art, Umfang und Dauer der Maßnahme genannt und der Sachverhalt inklusive einer Begründung dargestellt werden (§ 5a Abs. 3 HVSG). Auch die gerichtliche Anordnung muss detailliert werden (§ 5a Abs. 4 HVSG).²⁵⁹

(2) Sonderregelung für die Vorabkontrolle des Einsatzes von Verdeckten Mitarbeitern und Vertrauensleuten

Die allgemeinen Anforderungen an den Antrag auf Genehmigung und die Anordnung durch das Gericht gem. § 5a Abs. 3, 4 HVSG gelten für die Genehmigung des Einsatzes Verdeckter Mitarbeiter und Mitarbeiterinnen sowie von Vertrauenspersonen mit der Maßgabe, „dass Gegenstand von Antrag und Anordnung der Einsatz der verdeckten Mittel zur Aufklärung einer bestimmten nachrichtendienstlich beobachtungsbedürftigen Bestrebung oder Tätigkeit ist, ohne dabei konkrete verdeckte Mitarbeiterinnen oder Mitarbeiter oder Vertrauenspersonen zu benennen.“ Durch Auslegung des Geset-

²⁵⁹ Die Anforderungen an den Inhalt des Antrags und der Anordnung gem. § 5a Abs. 3, 4 [HVSG](#) seien aus dem neu gefassten § 46 Abs. 4, 5 BKAG übernommen worden, vgl. Drs. 20/10821 des Hessischen Landtags, S. 25.

zeswortlauts lässt sich nicht eindeutig feststellen, ob daneben die weiteren Anforderungen gem. § 5a Abs. 3,4 HVSG anwendbar sind. Aus der Gesetzesbegründung geht jedoch hervor, dass § 5a Abs. 5 HVSG nicht neben die allgemeinen Anforderungen tritt, sondern stattdessen anzuwenden ist. Demnach stellt „das anordnende Gericht in seinem Entscheidungstenor also lediglich fest, dass bestimmte Bestrebungen oder sicherheitsgefährdende oder geheimdienstliche Tätigkeiten bestimmter fremder Mächte durch dauerhaften Einsatz von Verdeckten Mitarbeiterinnen und Mitarbeitern oder Vertrauenspersonen aufgeklärt werden dürfen“. Das Gericht soll das „betreffende Beobachtungsobjekt“ „[f]reischalt[en]“; die eingesetzten Personen und konkreten Beschaffungsaufträge werden allerdings weder im Antrag noch in der Anordnung erwähnt (§ 5a Abs. 5 HVSG). Begründet wird diese Begrenzung mit der „Dauerhaftigkeit der Maßnahme“ und der in der Rechtsprechung angelegten Schutzpflicht gegenüber den eingesetzten Personen.²⁶⁰

Die Aufgabe des Vorabkontrolleurs ist, die Rechtmäßigkeit der Maßnahme festzustellen. Deshalb reicht es nicht aus, wenn das Gericht lediglich das „Beobachtungsobjekt“ freischaltet. Stattdessen muss es die Tatbestandsmäßigkeit und Verhältnismäßigkeit des Einsatzes prüfen. Hierfür benötigt es Informationen über den Einsatz. Während die Identität der eingesetzten Person grundsätzlich²⁶¹ wenig bedeutend ist und insoweit aus Geheimschutzgründen auch gegenüber dem Kontrolleur verschwiegen werden kann, muss das Gericht zumindest über die konkreten Beschaffungsaufträge informiert werden, denn die Eingriffsintensität variiert je nach Einsatzmodalität²⁶². Insoweit kommt es beispielsweise darauf an, wie häufig sich die Verdeckten Mitarbeiter oder Vertrauenspersonen mit den Betroffenen austauschen. Wenn sich die Eingriffsintensität ändert, ändert sich auch die Abwägung in der Verhältnismäßigkeit. Ein Gericht, dem nur Informationen über die aufzuklärende Bestrebung vorliegen, kann die Rechtmäßigkeit der Maßnahme somit nicht bewerten. Zudem muss der Vorabkontrolleur nach der Rechtsprechung des Bundesverfassungsgerichts über den Sachstand umfassend informiert werden, weshalb der Antrag der kontrollierenden Behörde substantiiert zu begründen ist.²⁶³

Im Ergebnis ist § 5a Abs. 5 HVSG verfassungswidrig, weil er verhindert, dass der Vorabkontrolleur umfassend informiert ist. Eine verfassungskonforme Vorabkontrolle

²⁶⁰ Drs. 20/10821 des Hessischen Landtags, S. 25; die Schutzpflicht spricht das Gericht jedoch nur hinsichtlich der Vertrauensleute an, BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 355.

²⁶¹ Dies kann anders zu beurteilen sein, wenn die Vertrauensperson beispielsweise aus dem familiären Umfeld der Zielperson stammt oder vorbestraft ist.

²⁶² Vgl. [Teil 2 A. III. 4. b. bb\) \(2\)](#).

²⁶³ BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 - 1 BvR 1140/09 - Rn. 117 f.; BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 215.

eingriffsintensiver Einsätze von Vertrauenspersonen und Verdeckten Mitarbeitern ist somit unmöglich.

(3) Keine Abschirmung des Gerichts

Der Gesetzesentwurf enthält keine Regelungen für eine räumliche Abschirmung des Gerichts. Zudem ist keine Sicherheitsüberprüfung des Geschäftsstellenpersonals bei Gericht vorgeschrieben.²⁶⁴ Diese Sicherheitsvorkehrungen müssen zwar nicht zwingend gesetzlich vorgesehen werden, die Gesetzesbegründung sollte jedoch einen Hinweis darauf enthalten, dass der Gesetzgeber eine Abschirmung als notwendig erachtet.

cc) Kernbereichsschutzvorkehrungen

Nach dem novellierten hessischen Verfassungsschutzgesetz ist das Amtsgericht zugleich „unabhängige Stelle“ zum Schutz des Kernbereichs privater Lebensgestaltung.²⁶⁵

dd) Beibehaltung der G 10-Kommission

Auch im Hessischen Verfassungsschutzgesetz ist die Vorabkontrolle auf zwei Kontrolleure aufgeteilt: Für die Genehmigung von Telekommunikationsüberwachungen und von besonderen Auskunftsverlangen ist die G 10-Kommission zuständig, für die Genehmigung des Einsatzes von IMSI-Catchern, längerfristigen Observationen und HUMINT das Amtsgericht.

Nach der Überarbeitung von § 16 G 10²⁶⁶ sollten die bisherigen Aufgaben der G 10-Kommission dem Amtsgericht übertragen und die G 10-Kommission aufgelöst werden. Somit würden unterschiedliche Kontrollniveaus vermieden und eine Konzentration der Vorabkontrolle bei einem Kontrolleur erreicht.

d. Faktoren für die gesetzliche Ausgestaltung

Bei der Übertragung der Vorabkontrolle eingriffsintensiver Maßnahmen auf Gerichte sollten folgende Aspekte bedacht werden:

²⁶⁴ Vgl. die bayerische Regelung auf [Teil 4 II. 3. b. bb](#)); ebenso „die Urkundsbeamten und das ganze Servicepersonal“, *Weisser*, DöV 2014, 831, 835.

²⁶⁵ § 7 Abs. 5, § 11 Abs. 7 [HVSG](#); vgl. auch Hessischer Landtag Drs. 20/10821 v. 21.3.2023, S. 27.

²⁶⁶ Vgl. [Teil 4 II. 1.](#)

aa) Zuständiges Gericht

Sowohl nach dem bayerischen als auch nach dem hessischen Verfassungsschutzgesetz soll das Amtsgericht am Sitz des Landesamts für Verfassungsschutz für die Genehmigung zuständig sein. Neben der ordentlichen Gerichtsbarkeit wäre es jedoch ebenso denkbar, diese Aufgabe der Verwaltungsgerichtsbarkeit zu übertragen, deren „Kernkompetenz typischerweise die Verwaltungskontrolle“ ist²⁶⁷.

bb) Ressourcen

Wenn die Vorabkontrolle aller eingriffsintensiven Maßnahmen dem Amtsgericht oder Verwaltungsgericht am Sitz der Verfassungsschutzbehörde übertragen wird, müssen dort zusätzliche Stellen geschaffen werden. Um den notwendigen Geheimschutz gewährleisten zu können, müssen zudem ausreichend Sachmittel zur Verfügung gestellt werden.²⁶⁸

cc) Räumliche Abschirmung des Gerichts

Da eine wirksame Spionageabwehr spätestens seit dem Angriffskrieg auf europäischem Boden und der offen feindlichen Haltung Russlands virulent geworden ist, wäre es unverantwortlich, die Kontrolleure auf der Landesebene (weiterhin) nicht abzuschirmen. Denn es besteht die Gefahr, dass feindlich gesinnte Akteure Daten, die bei den Nachrichtendiensten selbst ausreichend gesichert sind, über die Kontrolleure abschöpfen. Das ist jedoch kein Argument gegen Kontrollen an sich, sondern ein Argument für die Notwendigkeit effektiver Abschirmung im Bereich der Kontrolleure. Diese räumliche Abschirmung bedarf keiner gesetzlichen Grundlage, sie sollte aber zumindest Eingang in die Gesetzesbegründung finden.

dd) Personelle Abschirmung: Sicherheitsüberprüfung der Richter

In Zeiten, in denen selbst führende Beamte des BND trotz ihrer gründlichen Sicherheitsüberprüfung der Spionage überführt werden²⁶⁹, ist zu überlegen, ob in diesem eng umgrenzten Ausnahmebereich für Richter, die als Vorabkontrolleure der Nachrichtendienste agieren, eine Sicherheitsüberprüfung rechtfertigbar wäre. Auch wenn Spionage

²⁶⁷ Dietrich, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG, S. 22.

²⁶⁸ LT-Drs. 18/21537 v. 2.3.2022 https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwurf/%C3%84nderungsantrag_zum_gesetzentwurf_der_staatsregierung_zur_%C3%84nderung_des_bayerischen_verfassungsschutzgesetzes_und_des_bayerischen_datenschutzgesetzes.pdf (abgerufen am 31.8.2024), S. 18.

²⁶⁹ <https://www.zeit.de/news/2023-02/10/bnd-will-aus-russland-spionageaffaere-konsequenzen-ziehen> (abgerufen am 31.8.2024).

dadurch nicht sicher verhindert werden kann, wäre sie dennoch erschwert. Für das Erfordernis einer Sicherheitsüberprüfung von Richtern spricht zudem, dass auch bei der gerichtsähnlichen Kontrolle des UKRat auf der Bundesebene eine erweiterte Sicherheitsüberprüfung der Mitglieder vorgeschrieben worden ist (§ 43 Abs. 2 BNDG).

(1) Richterliche Unabhängigkeit gem. Art. 97 GG

Ein solches Vorhaben müsste jedoch mit Art. 97 GG vereinbar sein, der auch auf Richter der Länder anwendbar ist²⁷⁰. Gemeinsam mit Art. 92 Hs.1 GG, wonach die rechtsprechende Gewalt den Richtern übertragen ist, ist Art. 97 GG der „institutionell[e] Kern des grundgesetzlichen Rechtsstaatsprinzips“²⁷¹. Das Gebot der richterlichen Unabhängigkeit folgt darüber hinaus auch aus Art. 20 Abs. 2, 3 GG.²⁷²

Gem. Art. 97 Abs. 1 GG sind „Richter unabhängig und nur dem Gesetz unterworfen“. Auf die Norm können sich alle Richter berufen, unabhängig davon, ob sie haupt- oder ehrenamtlich tätig werden.²⁷³ Sie garantiert die sachliche Unabhängigkeit der Richter: erstens soweit diese rechtsprechend tätig werden, also eine Entscheidung treffen und vor- oder nachbereiten oder zweitens wenn sie Aufgaben übernehmen, die ihnen gerade wegen ihrer Unabhängigkeit übertragen wurden, beispielsweise im Rahmen der freiwilligen Gerichtsbarkeit.²⁷⁴ Art. 97 Abs. 1 GG ist jedoch nicht anwendbar, wenn Richter reine Verwaltungstätigkeiten ausüben.²⁷⁵ Dazu gehören beispielsweise die Betreuung von Referendaren, Tätigkeiten im Rechtshilfeverkehr²⁷⁶ und die Verwaltung von Justizvollzugsanstalten²⁷⁷.

Gegenüber der Exekutive schützt Art. 97 Abs. 1 GG vor Beeinflussung der rechtsprechenden Tätigkeit durch Weisungen²⁷⁸, durch Verwaltungsvorschriften oder vor sonstigen vermeidbaren Einflussnahmen.²⁷⁹ Davon erfasst sind auch Maßnahmen, die

²⁷⁰ Kahl/Waldhoff/Walter/Payandeh, Art. 97 GG Rn. 85.

²⁷¹ Epping/Hillgruber/Morgenthaler, Art. 97 GG Rn. 1.

²⁷² BVerfG, Beschluss v. 20.4.1982 – 2 BvL 26/81 – Rn. 144.

²⁷³ Kahl/Waldhoff/Walter/Payandeh, Art. 97 GG Rn. 131.

²⁷⁴ Sachs/Detterbeck, Art. 97 GG Rn. 11 a; Payandeh zählt dazu auch die Präsidiumstätigkeit, also beispielsweise die Aufstellung von Geschäftsverteilungsplänen, Kahl/Waldhoff/Walter/Payandeh, Art. 97 GG Rn. 133.

²⁷⁵ Zu dienstaufsichtlichen Befugnissen eines Richters, BVerfG, Beschluss v. 22.10.1974 – 2 BvR 147/70 – Rn. 50; Epping/Hillgruber/Morgenthaler, Art. 97 GG Rn. 5.

²⁷⁶ Kahl/Waldhoff/Walter/Payandeh, Art. 97 GG Rn. 134.

²⁷⁷ Epping/Hillgruber/Morgenthaler, Art. 97 GG Rn. 5.

²⁷⁸ BVerfG, Beschluss v. 24.3.1982 – 2 BvH 1/82 – Rn. 138.

²⁷⁹ Epping/Hillgruber/Morgenthaler, Art. 97 GG Rn. 10.

sich mittelbar auf die rechtsprechende Tätigkeit auswirken.²⁸⁰ Die Legislative muss dafür Sorge tragen, dass die Unabhängigkeit der Richter gesichert ist und dass ihre Gesetze die Exekutive nicht zu „vermeidbaren“ Möglichkeiten der Einflussnahme berechtigen.²⁸¹

Die Pflicht zur Sicherheitsüberprüfung würde sich auf die Richter beschränken, die mit der Aufgabe der Vorabkontrolle nachrichtendienstlicher Befugnisse betraut werden und daher Einblick in nachrichtendienstliche Informationen erlangen. Sollte das Ergebnis der Sicherheitsüberprüfung negativ ausfallen, käme der betroffene Richter für diese Aufgabe nicht in Betracht. In allen anderen Bereichen wäre er jedoch weiterhin einsetzbar. Die Sicherheitsüberprüfung wird daher zu Voraussetzung für die Ausübung eines bestimmten Bereichs der rechtsprechenden Tätigkeit. Da die Sicherheitsüberprüfung vor der Aufgabenzuweisung erfolgen würde, wäre dadurch jedoch kein bestimmtes gerichtliches Verfahren betroffen, weshalb ein Eingriff in die rechtsprechende Tätigkeit an sich zu verneinen ist. Aber selbst wenn ein Eingriff angenommen wird, wäre dieser nach der hier vertretenen Auffassung bei der aktuellen Sicherheitslage zum Schutz geheimhaltungsbedürftiger, nachrichtendienstlicher Informationen und damit der Funktionsfähigkeit der Nachrichtendienste unvermeidbar. Bei der einfachrechtlichen Ausgestaltung muss jedoch darauf geachtet werden, dass die Erkenntnisse der Sicherheitsüberprüfung nur zu diesem Zweck eingesetzt werden dürfen.

Anders als Art. 97 Abs. 1 GG garantiert Art. 97 Abs. 2 GG die persönliche Unabhängigkeit der hauptamtlichen und planmäßig angestellten Richter und schützt sie vor Amtsenthebung oder Versetzung gegen ihren Willen sowie vor anderen Eingriffen mit vergleichbaren Wirkungen.²⁸² Damit ist die persönliche Unabhängigkeit der Richter durch eine Sicherheitsüberprüfung nicht betroffen.

(2) § 2 Abs. 3 Nr. 2 SÜG

Nach dem einfachen Recht können Richter nicht sicherheitsüberprüft werden, „so weit sie Aufgaben der Rechtsprechung wahrnehmen“ (§ 2 Abs. 3 Nr. 2 SÜG sowie entsprechende Landesnormen²⁸³). Diese Privilegierung der Richter wirkt „funktionsbezo-

²⁸⁰ Kahl/Waldhoff/Walter/*Payandeh*, Art. 97 GG Rn. 133.

²⁸¹ BVerfG, Beschluss v. 7.1.1981 - 2 BvR 401/76 - Rn. 32; Sachs/*Detterbeck*, Art. 97 GG Rn. 9.

²⁸² Sachs/*Detterbeck*, Art. 97 GG Rn. 23 f., 35.

²⁸³ Vgl. z.B. Art. 2 Abs. 2 BaySÜG; § 2 Abs 3 Nr. 2 LSÜG BW; § 3 Abs. 3 Nr. 3 LSÜG RLP.

gen“ und gilt daher nicht, wenn ein Richter Verwaltungsaufgaben wahrnimmt, bei denen er Verschlusssachen einsieht.²⁸⁴ In dieser Funktion müssen auch Richter sicherheitsüberprüft werden.²⁸⁵ Damit wird die verfassungsrechtliche Unterscheidung zwischen der von Art. 97 Abs. 1 GG geschützten rechtsprechenden Tätigkeit und der nicht davon erfassten Wahrnehmung allgemeiner Verwaltungstätigkeiten im SÜG abgebildet.

Auf Sicherheitsüberprüfungen passt diese Unterscheidung jedoch nicht. Durch die Sicherheitsüberprüfung soll herausgefunden werden, ob: erstens Zweifel über die Zuverlässigkeit der Person bei der Wahrnehmung dieser Tätigkeit bestehen oder sie zweitens besonders gefährdet ist, sich beispielsweise durch fremde Nachrichtendienste erpressen zu lassen oder ob drittens Zweifel am Bekenntnis zur freiheitlich demokratischen Grundordnung oder dem Eintreten für deren Erhalten bestehen (§ 5 SÜG). Demzufolge wird die Person an sich überprüft, und zwar unabhängig davon, wegen welcher Funktion sie sich der Überprüfung unterziehen musste. Weil Bezugspunkt der Sicherheitsüberprüfung die Person ist, wirkt sie sich auch auf die Rechtsprechungsfunktion des Richters aus. Wenn man die Sicherheitsüberprüfung als vermeidbare und verfassungswidrige Beschränkung der richterlichen Unabhängigkeit erachtet, dürfte man allerdings gar keine Sicherheitsüberprüfung von Richtern zulassen.

Im Ergebnis ist es mit § 2 Abs. 3 Nr. 2 SÜG nicht vereinbar, für bestimmte richterliche Tätigkeiten eine Sicherheitsüberprüfung vorzusehen, denn dabei geht es um die Wahrnehmung von Rechtsprechungsaufgaben. Die Norm und vergleichbare Landesregelungen müssten deshalb angepasst werden, falls Sicherheitsüberprüfungen von Richtern in diesem eng begrenzten Ausnahmebereich als verfassungskonform erachtet werden.

4. Auflösung der Doppelzuständigkeit mit G 10-Kommission

In den Ländern, in denen die Vorabkontrolle eingriffsintensiver Maßnahmen einem Gericht übertragen wird, sollten die Aufgaben der G 10-Kommissionen ebenfalls diesem Gericht übertragen und die G 10-Kommissionen aufgelöst werden.²⁸⁶

²⁸⁴ *Warg*, Hdb. Sicherheits- und Staatsschutzrecht, 381, 401 Rn. 38; Schenke/Graulich/Rutwig/*Warg*, § 2 SÜG Rn. 16.

²⁸⁵ Allgemeine Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz SÜG-Ausführungsvorschrift (SÜG-AVV) vom 15. Februar 2018 (GMBI. S. 270) i.d.F. der mit Rundschreiben des Bundesministeriums des Innern und für Heimat vom 8. Juni 2022 S. 24, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/sueg-avv.pdf?__blob=publicationFile&v=5 (abgerufen am 31.8.2024).

²⁸⁶ Vgl. [Teil 4 II. 3. c. dd.](#)

5. Richter als „unabhängige Stellen“ für den Kernbereichsschutz

So wie in Bayern und Hessen bietet es sich auch in anderen Ländern an, die für die Vorabkontrolle zuständigen Gerichte zudem als unabhängige Stellen für den Kernbereichsschutz zu etablieren. Zur Vorbereitung und Beratung des Gerichts könnte dafür wie in Bayern eine „unterstützende Datenprüfstelle“ im LfV geschaffen werden.²⁸⁷ Die Einbindung von „ermittlungsspezifischem Fachverstand“ und „technische[r] Unterstützung“ hat das Bundesverfassungsgericht ermöglicht, soweit die externe Sichtung an „technische und fachliche Grenzen stößt“ und solange sichergestellt ist, dass die „Durchführung und Entscheidungsverantwortung“ bei der unabhängigen Stelle liegt.²⁸⁸

6. Datenschutzkontrollen durch die Landesdatenschutzbeauftragten

Die Landesdatenschutzbeauftragten sollen weiterhin für die laufenden Datenschutzkontrollen zuständig sein. Mit Auflösung der G 10-Kommissionen und Übertragung der Zuständigkeit auf die Datenschutzbeauftragten hätten diese einen potenziellen Kontroll-Gesamtüberblick über die Datenverarbeitungen des jeweiligen Verfassungsschutzes. Dafür müsste der für die Nachrichtendienstkontrolle bei den Landesdatenschutzbeauftragten vorgesehene Stellenanteil entsprechend erhöht werden²⁸⁹. Auch bei den Datenschutzkontrolleuren sollte niemand über Jahre hinweg allein für die Nachrichtendienstkontrolle zuständig sein, um eine zu starke institutionelle Nähe zu den Nachrichtendiensten und Missbrauch unwahrscheinlicher zu machen. Um das zu verhindern, wäre es denkbar, innerhalb der Datenschutzbehörden eine gemeinsame Zuständigkeit für die Kontrolle von Nachrichtendiensten und Polizei sowie Strafverfolgungsbehörden zu etablieren und die Zuständigkeiten der Mitarbeiter rotierend zu wechseln. Dies hätte den Vorteil, dass die Kontrollerfahrung aus den Kontrollen unterschiedlicher Behörden berücksichtigt werden könnte, sodass der Überblick sich sogar auf mehrere Sicherheitsbehörden erstrecken würde.

In den Fachgesetzen der Länder muss wie auf der Bundesebene ein Mindest-Kontrollintervall für die stichprobenartigen Datenschutzkontrollen etabliert werden²⁹⁰. Die Kontrollergebnisfolgen der Landesdatenschutzbeauftragten müssten nach diesem Kontrolldesign entsprechend derjenigen des BfDI gestärkt werden.²⁹¹

²⁸⁷ Vgl. Teil 3 E. III. 1.

²⁸⁸ BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17 - Rn. 315.

²⁸⁹ Vgl. [Teil 3 D. II. 4. a. bb\)](#), [Teil 3 D. II. 7. a.](#)

²⁹⁰ Vgl. [Teil 4. B. I. 4. b.](#)

²⁹¹ Vgl. [Teil 4. B. I. 4. c.](#)

7. Kontroll-Gesamtüberblick

Wie auf der Bundesebene sind auch in den Ländern die Datenschutzbeauftragten am ehesten geeignet, einen Kontroll-Gesamtüberblick zu erlangen. Um diesen zu realisieren, müssten auch in den Ländern die Ausnahmetatbestände gestrichen werden.²⁹²

Darüber hinaus müsste eine gesetzliche Regelung geschaffen werden, die es den Landesdatenschutzbeauftragten erlaubt, sich auszutauschen und zu kooperieren, soweit der jeweilige Kontrollgegenstand auf einer Kooperation der Nachrichtendienste beruht. Das Bundesverfassungsgericht hat sich in seiner Entscheidung zur Antiterrordatei bereits zur Zusammenarbeit von Kontrolleuren geäußert und festgehalten, dass der Gesetzgeber „auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen“ muss, wenn er eine „informationelle Kooperation der Sicherheitsbehörden“ vorsieht. Wegen der Ausgestaltung der Antiterrordatei als Verbunddatei müssten die Kontrolleure sich bei der Wahrnehmung ihrer Befugnisse gegenseitig unterstützen können.²⁹³

Dieser Gedanke ist auf alle gemeinsamen Dateien, gemeinsamen Zentren und Übermittlungsnormen übertragbar.

III. Fazit

Die Vorschläge für die Neugestaltung der externen Rechtskontrolle auf der Bundes- und Landesebene sind aus der Motivation heraus entstanden, ein verfassungskonformes Kontrolldesign zu erschaffen und trotzdem den Aufwand möglichst gering zu halten, indem neue Aufgaben nicht etwa an neu zu schaffende, sondern an bereits vorhandene Strukturen verteilt werden. Außerdem wird die Anzahl der zuständigen Kontrolleure reduziert, um die Nachrichtendienste zu entlasten.

Obwohl die rechtlichen Grundlagen den Ausgangspunkt funktionierender Rechtskontrolle markieren, darf nicht der Eindruck entstehen, dass ein mit höherrangigen Vorgaben zu vereinbarendes Kontrollregime zwangsläufig zu einer effektiven und wirksamen Nachrichtendienstkontrolle führt. Das rechtliche Kontrollregime ist nicht mehr als ein Grundgerüst, auf dem in der Praxis ein funktionierendes Kontrollverfahren aufbauen muss.²⁹⁴

²⁹² Vgl. [Teil 3 D. II. 7. b.](#)

²⁹³ BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07 - Rn. 216.

²⁹⁴ *Wetzling/Vieth*, Datenbasierte Nachrichtendienstkontrolle, S. 4; *Wetzling/Vieth*, Mehr Rechtskontrolle wagen, S. 19 ff.

Teil 5

Thesen

Teil 1

1. Der Gesetzgeber muss zur Ermöglichung der Rechtskontrolle bemüht sein, alle Befugnisse der Nachrichtendienste, die in Grundrechte eingreifen, normativ abzubilden und dafür eine gesetzliche Grundlage zu schaffen.
2. Die Intensität der Rechtmäßigkeitskontrolle von Tätigkeiten der Nachrichtendienste wird maßgeblich von der Ausgestaltung der diese Tätigkeit anleitenden Verhaltensnormen beeinflusst. Je eindeutiger die Befugnisnormen formuliert sind, desto detaillierter kann ihre Einhaltung kontrolliert werden. Soll die Rechtskontrolle verbessert werden, müssen die strukturell weiten Verhaltensnormen überarbeitet werden.
3. Dass die Nachrichtendienste der Rechtskontrolle bedürfen, ist ein Gebot der Gesetzmäßigkeit der Verwaltung, mithin des Rechtsstaatsprinzips. Die Heimlichkeit nachrichtendienstlicher Maßnahmen und die Tatsache, dass Betroffene in der Praxis häufig auch nachträglich nicht über die Beobachtung informiert werden, führen dazu, dass der Rechtskontrolle im Nachrichtendienstrecht umso größere Bedeutung zukommt.

Teil 2

4. Das Bundesverfassungsgericht hat aus den durch die nachrichtendienstliche Tätigkeit betroffenen Grundrechten verfassungsrechtliche Mindestanforderungen an die Rechtskontrolle entwickelt.
5. Die in der Rechtsprechung entwickelten Anforderungen werden grundrechtsübergreifend aus der Verhältnismäßigkeitsprüfung abgeleitet. Für die Bestimmung der konkreten verfassungsrechtlichen Anforderungen ist die Intensität des Eingriffs entscheidend.
6. Bei der externen Rechtskontrolle der Nachrichtendienste muss zwischen der Datenschutzaufsicht und der richterlichen oder richterähnlichen Vorabkontrolle differenziert werden.

7. Eine richterliche oder richterähnliche Vorabkontrolle ist nur bei schweren und besonders schweren Grundrechtseingriffen notwendig. Der Vorabkontrolleur muss „gerichtlich oder richterähnlich“ und unabhängig ausgestaltet sein. Er entscheidet in jedem Einzelfall und dauerhaft über die Zulässigkeit einer Maßnahme. Der Vorabkontrolleur muss über den Sachstand umfassend informiert werden, die ihm zur Entscheidung vorgelegten Anträge müssen substantiiert begründet und begrenzt sein. Ihm steht ein abschließendes Entscheidungsrecht zu. Der Vorabkontrolleur muss über die notwendige Sach- und Rechtskunde verfügen und so ausgestattet sein, dass er seine Aufgabe effektiv wahrnehmen kann. Die Third Party Rule darf die Vorabkontrolle nicht behindern.
8. Die Datenschutzaufsicht erstreckt sich auf alle nachrichtendienstlichen Maßnahmen. Welche Institution die Datenschutzaufsicht durchführt, kann der Gesetzgeber entscheiden. Die Stelle muss jedoch „unabhängig“ sein. Die Datenschutzkontrolle erfolgt punktuell und stichprobenartig. Dem Datenschutzkontrolleur müssen alle notwendigen Daten in praktikabel auswertbarer Weise zur Verfügung gestellt werden. Ihm müssen „wirksame“ Befugnisse zustehen. Der Datenschutzkontrolleur muss so ausgestattet werden, dass ihm regelmäßige Kontrollen möglich sind.
9. Die kontrollierenden Stellen müssen jedenfalls alle Maßnahmen, denen eine Person durch eine Behörde ausgesetzt ist, in den Blick nehmen können. Die Nachrichtendienstgesetze müssen eine Regelung enthalten, wonach mindestens einer der Kontrolleure alle Maßnahmen gegenüber einer Person überblicken kann und dementsprechend über einen „Kontrollgesamtüberblick“ verfügt.
10. Für die strategische Ausland-Fernmeldeaufklärung hat das Gericht detailliertere Anforderungen formuliert: Die Third Party Rule darf dieser Kontrolle nicht entgegenstehen. Die Datenschutzaufsicht soll laufend stichprobenartig prüfen. Der Datenschutzkontrolleur muss den Vorabkontrollen konsultieren können. Der Kontrollgegenstand und die Kontrollmittel der Kontrolleure sind detailliert beschrieben. Für die Besetzung gelten spezifische Vorgaben. Es müssen ausreichend Stellen und Mittel zur Verfügung gestellt werden. Zwischen dem Vorabkontrolleur und dem Datenschutzkontrolleur muss ein offener Austausch gewährleistet sein.
11. Davon unabhängig gilt für Maßnahmen mit Kernbereichsbezug das zweistufige Kernbereichsschutzkonzept, das auf der zweiten Stufe Kontrollen durch eine unabhängige Stelle vorsieht. Bei der Wohnraumüberwachung und dem Eingriff in informationstechnische Systeme (Online-Durchsuchung) müssen die Ergebnisse der Überwachung zwingend durch eine unabhängige Stelle gesichtet werden. Beim

Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern sowie bei der (Quellen-)Telekommunikationsüberwachung muss eine Sichtung durch eine unabhängige Stelle nicht in jeder Fallkonstellation erfolgen.

12. Die Annahme, dass der G 10-Kommission im Anwendungsbereich von Art. 10 GG ein ausschließliches Kontrollrecht zukommt, ist mit der neueren Rechtsprechung nicht mehr vertretbar.
13. Zur Beurteilung der Eingriffsintensität einer Maßnahme im Sicherheitsrecht hat das Bundesverfassungsgericht bestimmte Kriterien entwickelt. Es differenziert zwischen leichten, mittelschweren, schweren und besonders schweren Eingriffen.
14. Die nachrichtendienstlichen Standardbefugnisse bewirken überwiegend mindestens mittelschwere Eingriffe. Die meisten Befugnissen ermächtigen sogar zu „schweren“ oder „besonders schweren“ Eingriffen.
15. Bei der Beurteilung der Eingriffsintensität muss beachtet werden, dass der MAD häufig Soldaten bzw. Beamte überwacht. Dass diese Personen einer Verfassungstreuepflicht unterliegen und dem Staat berufsbedingt näherstehen als andere Personen, sollte bei der Bewertung der Eingriffsintensität bedacht werden. Dies gilt für die Beobachtung von Beamten und tariflich angestellten Mitarbeitern im öffentlichen Dienst gleichermaßen.
16. In der Rechtsprechung des Bundesverfassungsgerichts zur externen Rechtskontrolle liegt der Schwerpunkt auf der unabhängigen Vorabkontrolle. Weil die Vorabkontrolle die Erwartungen einer Kompensation der Heimlichkeit und der weiten Befugnisse nicht erfüllen kann, ist die Fokussierung des Bundesverfassungsgerichts auf diesen Kontrollzeitpunkt nicht nachvollziehbar.
17. Die Kehrseite der Fokussierung auf die Vorabkontrolle ist, dass das Bundesverfassungsgericht der laufenden bzw. nachträglichen Datenschutzkontrolle in seiner Rechtsprechung zum Nachrichtendienstrecht viel weniger Bedeutung beigemessen hat. Das ist mit Blick auf das Ziel der Kompensation fehlender Rechtsschutzmöglichkeiten Betroffener ein Fehler, weil die Informationen, die für die Beurteilung der Rechtmäßigkeit notwendig sind, erst bei der laufenden und nachträglichen Kontrolle vorliegen.
18. Indem das Bundesverfassungsgericht das gerichtsähnliche Kontrollorgan nicht nur als Rechtskontrolleur im eigentlichen Sinne begreift, sondern es mit der Aufgabe der Rechtsentwicklung betraut, überträgt es ihm eine quasi-gesetzgeberische Funktion und macht es zu einem sehr mächtigen Akteur. Deshalb ist es nicht nachvollziehbar, dass das Bundesverfassungsgericht keinerlei Vorkehrungen gegen einen potenziellen Machtmissbrauch des gerichtsähnlichen Kontrollorgans trifft.
19. Darüber hinaus schafft das Bundesverfassungsgericht in seiner Rechtsprechung Anreize für den Gesetzgeber, neue Kontrollstrukturen aufzubauen. In Anbetracht der bereits hohen Anzahl der Kontrolleure hätte das Bundesverfassungsgericht

diese Anreize mit der Vorgabe verbinden müssen, dass die Anzahl der Kontrolleure nicht erhöht werden darf.

20. Der EGMR unterscheidet „drei Stufen“ der Kontrolle, die nach ihrem Zeitpunkt unterschieden werden (ex ante, während der Durchführung, ex post). Für jede Stufe gelten bestimmte Vorgaben, die aber nicht per se verbindlich sind, sondern einander im Rahmen einer Gesamtbetrachtung unter Umständen ausgleichen können.
21. Die Vorabkontrolle muss unabhängig von der Exekutive ausgestaltet sein. In Eilfällen kann auf eine Genehmigung verzichtet werden, wenn sie innerhalb von 72 Stunden nachgeholt wird. Dem Kontrolleur müssen alle Dokumente vorgelegt werden, die er benötigt. Die Vorabkontrolle muss „effektiv“ sein.
22. Dass der Kontrolleur unabhängig sein muss, gilt auch für die Kontrolle während der Durchführung. Diese Kontrolle kann laufend oder stichpunktartig erfolgen. Der Kontrollierte muss die Anwendung geheimer Überwachungsmaßnahmen detailliert dokumentieren. Er muss rechtswidrige Datenverarbeitungen stoppen und anordnen dürfen, dass rechtswidrig erlangtes Material zerstört wird.
23. Die nachträgliche Kontrolle setzt voraus, dass der Betroffene über die Maßnahme benachrichtigt wird. Alternativ zur Benachrichtigung kann ein Rechtsweg vorgesehen werden, bei dem eine tatsächliche Betroffenheit nicht nachgewiesen werden muss.
24. Für anlasslose Telekommunikationsüberwachung gelten detailliertere Vorgaben. Der Zweck der Maßnahme und die für die Überwachung ausgewählten Träger der elektronischen Kommunikation, die Kommunikationsrouten und mindestens die Kategorien von Selektoren müssen im Genehmigungsantrag detailliert benannt werden. Der Kontrolleur auf der zweiten Stufe muss „ausreichend widerstandsfähig“ ausgestaltet sein. Grundsätzlich müsse auf jeder Stufe ein anderer Kontrolleur zuständig sein.
25. Der EuGH hat in jüngeren Entscheidungen zwei unterschiedliche Definitionen zum Begriff der „nationalen Sicherheit“ verwendet. Welche der beiden Definitionen maßgeblich ist, bleibt abzuwarten. Die ausführliche Definition des EuGH zur „nationalen Sicherheit“ gem. Art. 4 Abs. 2 S. 3 EUV hat zur Folge, dass die Tätigkeiten der Nachrichtendienste nicht länger generell unter Art. 4 Abs. 2 S. 3 EUV subsumiert werden können und damit zum Teil in den Anwendungsbereich des Unionsrechts fallen:
 - Da die politische Unterrichtung der Bundesregierung sich auch auf wirtschaftliche und kulturelle Vorgänge von außen- und sicherheitspolitischer Bedeutung erstrecken kann und der Auftrag des BND somit nicht auf die Verhütung von Bedrohungen begrenzt ist, fällt dessen Tätigkeit zum Teil in den Anwendungsbereich des Unionsrechts.

- Soweit die Landesämter für Verfassungsschutz nicht ausschließlich besonders schweren Erscheinungsformen der organisierten Kriminalität beobachten, fällt diese Beobachtung in den Anwendungsbereich des Unionsrechts.
 - Je nach Auslegung des Begriffs der „unmittelbaren“ Bedrohung fallen weite Teile der nachrichtendienstlichen Vorfeldaufklärung in den Anwendungsbereich des Unionsrechts.
26. Die Öffentlichkeitsarbeit sowie sonstige Prävention durch die Verfassungsschutzbehörden fallen ebenfalls in den Anwendungsbereich des Unionsrechts.
 27. Auf die Bestandteile der nachrichtendienstlichen Tätigkeit, die nunmehr in den Anwendungsbereich des Unionsrechts fallen, sollte grundsätzlich die souveränitätsschonendere JIRL angewandt werden.
 28. Soweit die Nachrichtendienste allerdings im Einzelfall nicht zum Zweck der Gefahrenabwehr mit potenziellem Straftatbezug oder zur Strafverfolgung handeln, sondern ihre Tätigkeit mit „allgemeiner Gefahrenabwehr“ vergleichbar ist, fällt diese Tätigkeit in den Anwendungsbereich der DSGVO. Wenn der Verfassungsschutz beispielsweise automatisiert Daten verarbeitet, um in Schulen oder anderen Einrichtungen Fortbildungen und Fachtagungen zu Präventionszwecken anzubieten, besteht kein potenzieller Straftatbezug.
 29. Gem. Art. 47 Abs. 1 JIRL sind alle Aufsichtsbehörden mit „wirksamen Untersuchungsbefugnissen“ auszustatten. Davon ist zumindest die Befugnis erfasst, Zugang zu den für die Aufgabenerfüllung notwendigen Informationen zu erhalten. Darüber hinaus müssen die Mitgliedstaaten gem. Art. 47 Abs. 2 JIRL vorsehen, dass jede Aufsichtsbehörde über „wirksame Abhilfebefugnisse“ verfüge. Wirksam sind die Befugnisse nur, wenn sie verbindlich wirken, der Verantwortliche also daran gebunden ist.
 30. Im Anwendungsbereich der DSGVO stehen den datenschutzrechtlichen Aufsichtsbehörden weitreichendere Abhilfebefugnisse zur Verfügung: Gem. Art. 58 Abs. 2 DSGVO können sie gegenüber dem Verantwortlichen unter anderem Verarbeitungsverbote erteilen.
 31. Soweit die vollharmonisierende DSGVO einschlägig ist, sind die Unionsgrundrechte zu beachten. Soweit im mitgliedstaatlichen Recht Ausnahmen von Betroffenenrechten der JIRL normiert oder die Normen über die Aufsichtsbehörden umgesetzt werden, wird Unionsrecht durchgeführt, sodass die Grundrechtecharta ebenfalls anwendbar ist.
 32. Art. 8 Abs. 2 S. 2 GRCh verleiht dem Einzelnen das Recht, Auskunft über die Verarbeitung personenbezogener Daten zu erhalten und Berichtigung oder Löschung dieser Daten verlangen zu können. Gem. Art. 8 Abs. 3 GRCh muss die Einhaltung des Datenschutzes von unabhängigen, weisungsfreien Stellen überwacht werden.

Darüber hinaus kann das Recht auf einen wirksamen Rechtsbehelf gem. Art. 47 GRCh zu beachten sein.

33. Der EuGH hat bisher nicht über nachrichtendienstliche Datenverarbeitungen durch Mitgliedstaaten geurteilt. Es gab jedoch Entscheidungen mit Bezügen dazu: So hat er in den Entscheidungen zur Vorratsdatenspeicherung Kontrollvorgaben formuliert. Bei der Sammlung von Standort- und Verkehrsdaten in Echtzeit muss eine Vorabkontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle vorgesehen werden, deren Entscheidung bindend ist und die prüft, dass die Datenverarbeitung die Grenzen des „absolut notwendigen“ nicht überschreitet. Aus Schrems II ergibt sich, dass eine auf die konkrete Zielperson (oder den konkreten Selektor) bezogene Genehmigung oder Aufsicht einer unabhängigen Stelle gegeben sein muss und Betroffene über Rechtsbehelfe verfügen müssen, auf deren Grundlage sie vor einem unabhängigen Organ die Auskunft über die Verarbeitung sowie die Löschung oder Berichtigung ihrer personenbezogenen Daten verlangen können.
34. Dass als Folge der Anwendung der Definition des EuGH das Unionsrecht einerseits gar nicht einschlägig ist, andererseits jedoch die JIRL und am Rande die DSGVO anzuwenden sind, stellt den Gesetzgeber vor eine komplizierte Aufgabe. In Bezug auf die externe Rechtskontrolle der Nachrichtendienste besteht eine denkbare unionsrechtskonforme Lösungsoption darin, die Befugnisse der Datenschutzaufsicht generell aus Art. 47 JIRL herzuleiten.

Teil 3

35. Insgesamt müssen für eine Vielzahl nachrichtendienstlicher Befugnisse von (besonders) schwerer Eingriffsintensität bundesweit überhaupt erst unabhängige Vorabkontrollen eingeführt werden. Dies betrifft die langfristigen Observationen, den Einsatz von Verdeckten Ermittlern oder Vertrauenspersonen und den Einsatz technischer Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkgerätes oder zur Ermittlung der Geräte- oder Kartennummer.
36. Vorab genehmigte Eilanordnungen sind konventionswidrig, wenn die Genehmigung der G 10-Kommission nicht oder zu spät nachgeholt wird. Eine rein ehrenamtliche Tätigkeit der Mitglieder der G 10-Kommissionen kann der verfassungsrechtlichen Anforderung der Wirksamkeit der Kontrolle nicht gerecht werden. Dass die Mitglieder der G 10-Kommissionen unbegrenzt wiedergewählt werden können, ist verfassungswidrig. Die G 10-Kommissionen verfügen insgesamt nicht über die verfassungsrechtlich „notwendige“ Personal- und Sachausstattung.
37. Die Vorabkontrolle des UKRat ist insoweit konventionswidrig, als dass sie keine unabhängige Vorabkontrolle der Selektoren bzw. zumindest von Kategorien von

Selektoren vorsieht, sondern lediglich eine ex post-Kontrolle durch das administrative Kontrollorgan etabliert. Da die Suchbegriffe für die gezielte Datenerhebung in der Anordnung nicht benannt werden müssen, kann das gerichtsähnliche Kontrollorgan diese Suchbegriffe nicht kontrollieren, was verfassungswidrig ist. Die Protokollierungspflichten des BND gehen in konventions- und verfassungswidriger Weise nicht weit genug. Dass der UKRat für die Einsichtnahme in Original-Akten ein berechtigtes Interesse geltend machen muss, ist mit der Rechtsprechung des Bundesverfassungsgerichts nicht vereinbar. Um die verfassungsrechtlichen Vorgaben zu erfüllen, müsste gesetzlich geregelt werden, dass das administrative Kontrollorgan unter anderem aus Personen mit „informationstechnischen Kenntnissen“ bestehen muss. Insoweit die Third Party Rule für den UKRat wie eine Kontrollbarriere wirkt, da der Zugang zu informationstechnischen Systemen bzw. der Zugang zu Diensträumen verwehrt wird, weil keine alleinige Verfügungsbeziehung des BND besteht, ist die Rechtslage verfassungswidrig.

38. In Mecklenburg-Vorpommern existiert keine Norm, die die Zuständigkeit des LfDI für die Datenschutzkontrolle beim Verfassungsschutz festlegt. Das ist verfassungswidrig. Selbst wenn man annimmt, die Zuständigkeit sei herleitbar, ist zumindest verfassungswidrig, dass der LfDI weder über Kontrollmittel zur Informationsgewinnung noch über Kontrollergebnisfolgen verfügt.
39. In vielen Ländern ist für die Datenschutzkontrolle der Verfassungsschutzbehörden keine ausreichende Stellenanzahl vorgesehen, die ihnen „regelmäßige“ Kontrollen ermöglichen würden. Das ist verfassungswidrig.
40. Der in manchen Gesetzen vorgesehene vollständige Ausschluss der Kontrollrechte ist verfassungswidrig.
41. Die Beanstandung ist keine „wirksame Befugnis“ im Sinne der Rechtsprechung. Alle Fachgesetze, in denen das schwache Instrument der Beanstandung die effektivste Kontrollergebnisfolge ist, sind daher verfassungswidrig. Soweit die nachrichtendienstliche Tätigkeit in den Anwendungsbereich des Unionsrechts fällt, ist die Ausstattung mit dem unverbindlichen Beanstandungsrecht zusätzlich unionsrechtswidrig.
42. Die Verfassungsschutzgesetze von Berlin und Mecklenburg-Vorpommern enthalten kein Kernbereichsschutzkonzept und sind daher verfassungswidrig.
43. Das Verfassungsschutzgesetz von Sachsen-Anhalt sieht auf der Auswertungsebene keine Sichtung durch eine unabhängige Stelle vor, obwohl es zur Wohnraumüberwachung ermächtigt. Das ist verfassungswidrig. Dass das Verfassungsschutzgesetz von Schleswig-Holstein beim Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten auch in Zweifelsfällen keine Kontrolle vorsieht, macht das Kernbereichsschutzkonzept verfassungswidrig.

44. Sechs Verfassungsschutzgesetze sehen zwar eine Sichtung vor, die Stelle ist dort jedoch nicht unabhängig vom Nachrichtendienst. Das ist verfassungswidrig.
45. Die Rechtslage auf der Bundesebene, in Baden-Württemberg und Bremen ist insoweit verfassungswidrig, weil eine unabhängige Sichtung bei kernbereichsrelevanten Daten aus der Wohnraumüberwachung nicht vorgesehen ist, obwohl diese Nachrichtendienste dazu befugt sind.
46. Dass in Brandenburg, Rheinland-Pfalz und dem Saarland die unabhängigen Stelle bei der Wohnraumüberwachung und der Online-Durchsuchung nicht immer, sondern nur dann eingebunden werden muss, wenn Zweifel bestehen, ob die erhobenen Daten kernbereichsrelevant sind, macht diese Regelungen verfassungswidrig.

Teil 4

47. Das gerichtsähnliche Kontrollgremium des UKRat sollte für die Vorabkontrolle aller eingriffsintensiven Maßnahmen der Nachrichtendienste des Bundes zuständig sein.
48. Für die nachträgliche Rechtmäßigkeitskontrolle sollte der BfDI zuständig sein.
49. Da die bisherigen Aufgaben der G 10-Kommission nach diesem Vorschlag durch den UKRat und den BfDI wahrgenommen werden, besteht für die G 10-Kommission keine Notwendigkeit mehr, sodass sie aufgelöst werden kann.
50. Wenn der UKRat für die Vorabkontrolle aller eingriffsintensiven nachrichtendienstlichen Mittel zuständig ist, ergibt seine Regelung (ausschließlich) im BNDG keinen Sinn mehr. Stattdessen sollte der Auftrag des UKRat in einem separaten Gesetz detailliert werden. Dabei können die Normen des BNDG grundsätzlich übernommen werden, wobei im Detail Änderungen notwendig sind.
51. Bei der Reform der Rechtskontrolle sollten die bestehenden verfassungsrechtlichen Defizite der Kontrolle durch den BfDI behoben werden: Das Kontrollintervall müsste gesetzlich verkürzt, die Kontrollergebnissefolgen müssten verstärkt und die Kontrollbarrieren abgebaut werden.
52. Wie auf der Bundesebene wird auch für die Länder die Auflösung der G 10-Kommissionen vorgeschlagen.
53. Auf der Landesebene sollte die Vorabkontrolle dem Amtsgericht oder Verwaltungsgericht am Amtssitz des Landesamtes für Verfassungsschutz übertragen werden. An den jeweiligen Gerichten müssen dafür zusätzliche Stellen geschaffen und für eine wirksame Abschilderung gesorgt werden. Die Aufgaben der G 10-Kommissionen sollten ebenfalls diesem Gericht übertragen werden, um eine Aufspaltung der Kontrolle zu verhindern. Die für die Vorabkontrolle zuständigen Gerichte sollten zudem als unabhängige Stellen für den Kernbereichsschutz etabliert werden.

Die Defizite der Kontrolle durch die Landesdatenschutzbeauftragten müssen behoben werden.

Literaturverzeichnis

- Aden, Hartmut*, Datenschutzkontrolle auf Bundesebene- unabhängig und effektiver?, Vorgänge 2015, 245–250.
- Ader, Werner*, § 19 Struktur und Prozesse der Auslandsaufklärung, in: Jan-Hendrik Dietrich, Matthias Fahrner, Nikolaos Gazeas et al. (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, München 2022, S. 612–666.
- Alt, Frederike*, Kompensatorische Kontrolle heimlicher Grundrechtseingriffe, Entwicklung einer sicherheitsrechtlichen Kontrolldogmatik unter besonderer Berücksichtigung administrativer Kontrollstrukturen, Tübingen 2024.
- Anderson, David*, A question of trust, Report of the Investigatory Powers Review, Independent Reviewer of Terrorism Legislation 2015, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>, Stand: Juni 2015. Zuletzt abgerufen am: 31.08.2024.
- Arndt, Claus*, Das G 10-Verfahren, in: Bundesministerium des Innern (Hrsg.), Verfassungsschutz und Rechtsstaat, Köln u.a. 1981, S. 43–64.
- Arnim, Hans Herbert von*, Grundragen der Kontrolle von Gesetzgebung und Verwaltung, DöV 1982, 917–925 (zitiert: *Arnim*, DöV 1982).
- Arnim, Hans Herbert von*, Kontrolle, in: Werner Heun, Martin Honecker, Martin Morlok et al. (Hrsg.), Evangelisches Staatslexikon, Neuausgabe, Stuttgart 2006, S. 1316–1319 (zitiert: *Arnim*, Kontrolle 2006).
- Aust, Helmut Philipp*, Auslandsaufklärung durch den Bundesnachrichtendienst, DöV 2020, 715–724.
- Aust, Helmut Philipp*, Spionage im Zeitalter von Big Data- Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht, Archiv des Völkerrechts 2014, 375–406.
- Bäcker, Matthias*, § 28 Sicherheitsverfassungsrecht, in: Matthias Herdegen, Johannes Masing, Ralf Poscher et al. (Hrsg.), Handbuch des Verfassungsrechts, Darstellung in transnationaler Perspektive, München 2021, S. 1715–1783 (zitiert: *Bäcker*, Hdb. des Verfassungsrechts 2021).
- Bäcker, Matthias*, Beschwerdeschrift Verfassungsbeschwerde gegen das Bayerische Verfassungsschutzgesetz, 21.7.2017 (zitiert: *Bäcker*, Beschwerdeschrift BayVSG).
- Bäcker, Matthias*, Beschwerdeschrift Verfassungsbeschwerde gegen das BNDG, 19.12.2017 (zitiert: *Bäcker*, Beschwerdeschrift BNDG).
- Bäcker, Matthias*, Beschwerdeschrift- Verfassungsbeschwerde gegen das G 10 (zitiert: *Bäcker*, Beschwerdeschrift G 10).
- Bäcker, Matthias*, Beschwerdeschrift, Verfassungsbeschwerde gegen das BNDG in der Fassung vom 19. April 2021, 2022 (zitiert: *Bäcker*, Beschwerdeschrift BNDG II).
- Bäcker, Matthias*, Das G 10 und die Kompetenzordnung, DöV 2011, 840–848 (zitiert: *Bäcker*, DöV 2011).
- Bäcker, Matthias*, Das Grundgesetz als Implementationsgarant der Unionsgrundrechte, EuR 2015, 389–413 (zitiert: *Bäcker*, EuR 2015).

- Bäcker, Matthias*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hermann Hill, Dieter Kugelman, Mario Martini (Hrsg.), Perspektiven der digitalen Lebenswelt, Baden-Baden 2017, S. 63–88 (zitiert: *Bäcker*, Datenschutzrichtlinie für Polizei und Strafjustiz).
- Bäcker, Matthias*, Kriminalpräventionsrecht, Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, Tübingen 2015 (zitiert: *Bäcker*, Kriminalpräventionsrecht).
- Bäcker, Matthias*, Organisationsverfassungsrechtliche Grundlagen des Polizeirechts, in: Erhard Denninger, Matthias Bäcker, Kurt Graulich (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr-Strafverfolgung - Rechtsschutz, 7. Aufl., Köln 2021, S. 109–164 (zitiert: *Bäcker*, Hdb. des Polizeirechts).
- Bäcker, Matthias*, Stellungnahme zu dem Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041) v. 23.09.2016, Deutscher Bundestag, Innenausschuss, Ausschussdr. 18(4)653 G (zitiert: *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des BND).
- Bäcker, Matthias*, Strategische Telekommunikationsüberwachung auf dem Prüfstand, K&R 2014, 556–561 (zitiert: *Bäcker*, K&R 2014).
- Bäcker, Matthias*, Weitere Zentralisierung der Terrorismusbekämpfung?, GSZ 2018, 213–219 (zitiert: *Bäcker*, GSZ 2018).
- Bäcker, Matthias*, Zur Reform der Eingriffstatbestände im Nachrichtendienstrecht, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich et al. (Hrsg.), Nachrichtendienste im demokratischen Rechtsstaat, Tübingen 2018, S. 137–151 (zitiert: *Bäcker*, Eingriffstatbestände).
- Backes, Otto/Gusy, Christoph*, Wer kontrolliert die Telefonüberwachung?, Frankfurt am Main 2003 (zitiert: *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?).
- Badura, Peter*, Die Legitimation des Verfassungsschutzes, in: Bundesamt für Verfassungsschutz (Hrsg.), Verfassungsschutz in der Demokratie, 1990, S. 27–51 (zitiert: *Badura*, Legitimation des Verfassungsschutzes).
- Baker, Stewart*, How Can the U.S. Respond to Schrems II?, <https://www.lawfareblog.com/how-can-us-respond-schrems-ii>; Stand: Juli 2020. Zuletzt abgerufen am: 31.8.2024.
- Banse, Dirk/Büscher, Wolfgang/Kraetzer, Ulrich/Müller, Uwe*, Das Kreuz mit der Kontrolle, Was darf ein Geheimdienst und wie wird er kontrolliert? Über diese Frage ist im politischen Berlin eine Kontroverse entbrannt. Ein geplantes Gesetz ist vorerst gestoppt, Welt am Sonntag vom 27.08.2023.
- Bantlin, Franziska*, Die G 10-Kommission - zur Kontrolle der Nachrichtendienste, Schriften zum öffentlichen Recht Band 1452, Berlin 2021 (zitiert: *Bantlin*, G 10-Kommission).
- Bantlin, Franziska*, Grundrechtsschutz bei Telekommunikationsüberwachung und Online-Durchsuchung, JuS 2019, 669–673 (*Bantlin*, JuS 2019).
- Bantlin, Franziska*, »Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung« - Bericht über das 2. Symposium zum Recht der Nachrichtendienste in Berlin, DVBl 2018, 925–927 (zitiert: *Bantlin*, DVBl 2018).
- Bantlin, Franziska/Graulich, Kurt*, Aktuelle Rechtsprechung des Bundesverfassungsgerichts und daraus folgende Reformfordernisse für die Nachrichtendienstkontrolle, GSZ 2023, 179–183.

- Banzhaf, Maximilian*, Die Ämter für Verfassungsschutz als Präventionsbehörden, Rechtsfragen zur Stellung der Verfassungsschutzämter in der deutschen Verfassungsschutzarchitektur, Berlin 2021.
- Barczak, Tristan*, Das Recht der Nachrichtendienste: Missstände, Entwicklungen und Perspektiven eines Rechtsgebiets in der Findungsphase, *KritV* 2021, 91–134 (zitiert: *Barczak*, *KritV* 2021).
- Barczak, Tristan*, Nachrichtendienstliche Beobachtung internationaler extremistischer Netzwerke, Mehr als eine Zuständigkeitsfrage?, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich et al. (Hrsg.), Radikalisierung und Extremismus, Aufgabenfelder und Herausforderungen der Nachrichtendienste, Tübingen 2023, S. 193–217 (zitiert: *Barczak*, Nachrichtendienstliche Beobachtung 2023).
- Barczak, Tristan*, Vom rechtsfreien Raum zum raumlosen Recht?, Anmerkungen zum BND-Urt. des Bundesverfassungsgerichts vom 19. Mai 2020, 1 BvR 2835/17, BayVbl 2020, 685–692 (zitiert: *Barczak*, BayVbl 2020).
- Bareinske, Christian*, Auslandsaufklärung, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 865–933.
- Bartodziej, Peter*, Parlamentarische Kontrolle, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 1533–1606.
- Baumgartner, Annina*, Anmerkung zu EuGH, Urt. vom 6.10.2020, C-623/17 (Privacy International), *GSZ* 2021, 42–44.
- Bäumler, Helmut*, Der Auskunftsanspruch des Bürgers gegenüber den Nachrichtendiensten, *NVwZ* 1988, 199–205 (zitiert: *Bäumler*, *NVwZ* 1988).
- Bäumler, Helmut*, Wahrung der Grundrechte durch Datenschutzbeauftragte, *RDV* 1996, 163–169 (zitiert: *Bäumler*, *RDV* 1996).
- Bergemann, Nils*, Die Freiheit im Kopf? – Neue Befugnisse für die Nachrichtendienste, Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, *NVwZ* 2015, 1705–1710.
- Bergemann, Nils*, Nachrichtendienste und Polizei, in: Erhard Denninger, Matthias Bäcker, Kurt Graulich (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl., Köln 2021, S. 1225–1301 (zitiert: *Bergemann*, Hdb. des Polizeirechts).
- Bernstorff, Jochen von/Asche, Josephine*, Nachrichtendienste und Menschenrechte, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 79–106.
- Bewarder, Manuel/Flade, Florian*, Lauschangriff? Erlaubt! <https://www.tagesschau.de/investigativ/ndr-wdr/bnd-unabhaengiger-kontrollrat-101.html>; Stand: April 2023. Zuletzt abgerufen am: 31.8.2024 (zitiert: *Bewarder/Flade*, Lauschangriff).
- Bewarder, Manuel/Flade, Florian*, Machtkampf unter BND-Kontrolleuren, Streit über Ausrichtung, <https://www.tagesschau.de/investigativ/ndr-wdr/bnd-unabhaengiger-kontrollrat-102.html>; Stand: März 2023. Zuletzt abgerufen am: 31.8.2024 (zitiert: *Bewarder/Flade*, Machtkampf).
- Bewarder, Manuel/Flade, Florian*, Wer überwacht die Überwacher?, <https://www.tagesschau.de/investigativ/ndr-wdr/unabhaengiger-kontrollrat-101.html>; Stand: Februar 2023. Zuletzt abgerufen am: 31.08.2024 (*Bewarder/Flade*, Überwacher).
- Bignami, Francesca*, Schrems II: The Right to Privacy and the New Illiberalism, <https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism/>; Stand: Juli 2020. Zuletzt abgerufen am: 31.08.2024.

- Binder, Reinhart/Vesting, Thomas* (Hrsg.), Beck'scher Kommentar zum Rundfunkrecht, 5. Aufl., München 2024 (zitiert: *Binder/Vesting/Bearbeiter*).
- Böckenförde, Ernst-Wolfgang*, § 34 I. Legitimation, Amt, Form, in: Josef Isensee, Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3., völlig neu bearbeitete und erweiterte Auflage, Juris, Heidelberg u.a. 2003 (zitiert: *Böckenförde*, Hdb. des Staatsrechts 2003).
- Bonin, Irina*, Grundrechtsschutz durch verfahrensrechtliche Kompensation bei Maßnahmen der polizeilichen Informationsvorsorge, Stuttgart u.a. 2012.
- Borgers, Michael*, Als die Massenüberwachung öffentlich wurde, Zehn Jahre NSA-Affäre, 05.06.2023, <https://www.deutschlandfunk.de/zehn-jahre-nsa-affaere-100.html>; Stand: Juni 2023. Zuletzt abgerufen am: 31.8.2024.
- Borgs-Maciejewski, Hermann*, Parlament und Nachrichtendienste, Die unzulängliche Kontrolle der geheimen Nachrichtendienste, <https://www.bpb.de/shop/zeitschriften/apuz/archiv/530389/parlament-und-nachrichtendienste-die-unzulaengliche-kontrolle-der-geheimen-nachrichtendienste/>; Stand: Februar 1977. Zuletzt abgerufen am: 31.08.2024.
- Botta, Jonas*, Eine Frage des Niveaus: Angemessenheit drittstaatlicher Datenschutzregime im Lichte der Schlussanträge in „Schrems II“, Der Prüfungsmaßstab der Gleichwertigkeit und seine Reichweite im Bereich der nationalen Sicherheit, CR 2020, 82–89.
- Brandt, Karsten*, Öffentlichkeitsarbeit durch Nachrichtendienste, in: Jan-Hendrik Dietrich, Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 1709–1763.
- Brenner, Michael*, Bundesnachrichtendienst im Rechtsstaat, Zwischen geheimdienstlicher Effizienz und rechtsstaatlicher Kontrolle, Baden-Baden 1990.
- Breuer, Marten*, § 25 Datenschutz, in: Sebastian Heselhaus, Carsten Nowak (Hrsg.), Handbuch der Europäischen Grundrechte, 2. Aufl., München 2020, S. 549–568.
- Brunner, Georg*, Kontrolle in Deutschland : eine Untersuchung zur Verfassungsordnung in beiden Teilen Deutschlands, Köln 1972.
- Bull, Hans Peter*, Datenschutz und Ämter für Verfassungsschutz, in: Bundesministerium des Innern (Hrsg.), Verfassungsschutz und Rechtsstaat, Köln u.a. 1981, S. 133–156 (zitiert: *Bull*, Datenschutz).
- Bull, Hans Peter*, Sind Nachrichtendienste unkontrollierbar?, Zu der Diskussion über die parlamentarische Kontrolle des Einsatzes nachrichtendienstlicher Mittel am Beispiel Sachsen, DöV 2008, 751–759 (zitiert: *Bull*, DöV 2008, 751).
- Bundesbeauftragte für den Datenschutz*, Sachstandsbericht (Stand: 30. Juli 2015) – rechtliche Bewertung, Datenschutzrechtliche Beratung und Kontrolle gemäß § 24 und § 26 Absatz 3 Bundesdatenschutzgesetz der Erhebung und Verwendung personenbezogener Daten in bzw. in Zusammenhang mit der Dienststelle des BND in Bad Aibling, <https://netzpolitik.org/2016/geheimerprueferbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/#Sachstandsbericht>; Stand: September 2016. Zuletzt abgerufen am: 31.08.2024 (zitiert: *BfDI*, Sachstandsbericht).
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, Das Militärische Nachrichtenwesen – ein Nachrichtendienst ohne Regeln?, <https://background.tagesspiegel.de/cybersecurity/das-militaerische-nachrichtenwesen-ein-nachrichtendienst-ohne-regeln>; Stand: Oktober 2023. Zuletzt abgerufen am: 31.08.2024 (zitiert: *BfDI*, Das Militärische Nachrichtenwesen).

- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, Stellungnahme zum Gesetzentwurf der Bundesregierung zur Änderung des BND-Gesetzes v. 18.12.2020, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdrs. 19(4)682 (zitiert: *BfDI*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG).
- Callies, Christian/Ruffert, Matthias* (Hrsg.), EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 6. Aufl., München 2022.
- Cameron, Iain*, European Union Law Restraints on Intelligence Activities, *International Journal of Intelligence and Counterintelligence* 2020, 452–463.
- Cameron, Iain*, National Security and the European Convention on Human Rights, 2000 (zitiert: *Cameron*, National Security).
- Cameron, Iain*, Oversight of Intelligence Agencies, The European Dimension, in: Zachary K. Goldman, Samuel J. Rascoff (Hrsg.), *Global Intelligence Oversight, Governing Security in the twenty-first century*, New York 2016, S. 71–93 (zitiert: *Cameron*, Oversight of Intelligence Agencies).
- Conrad, Gerhard*, Situational Awareness for EU Decision-making: The Next Decade, *European Foreign Affairs Review* 2021, 55–70.
- Crespi, Serena*, The Applicability of Schrems Principles to the Member States: National Security and Data Protection within the EU Context, *European Law Review* 2018, 669–686.
- Deiseroth, Dieter*, Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf?, *ZRP* 2013, 194–197.
- Denninger, Erhard*, Das Recht auf informationelle Selbstbestimmung und innere Sicherheit, Folgerungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts, *KJ* 1985, 215–244 (zitiert: *Denninger*, *KJ* 1985).
- Denninger, Erhard*, Verfassungsschutz, Polizei und die Bekämpfung der Organisierten Kriminalität, *KritV* 1994, 232–241 (zitiert: *Denninger*, *KritV* 1994).
- Deutscher Anwaltverein*, Stellungnahme zum Regierungsentwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 25.1.2021, März 2021, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschuss-Drs. 19(4)731 I (zitiert: *Deutscher Anwaltverein*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG).
- Dietrich, Jan-Hendrik*, § 3 Das Recht der Nachrichtendienste, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), *Handbuch des Rechts der Nachrichtendienste*, Stuttgart 2017, S. 249–293 (zitiert: *Dietrich*, *Hdb. des Rechts der Nachrichtendienste*, 249).
- Dietrich, Jan-Hendrik*, Geheime Mitarbeiter der Nachrichtendienste, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), *Handbuch des Rechts der Nachrichtendienste*, Stuttgart 2017, S. 1017–1091 (zitiert: *Dietrich*, *Hdb. des Rechts der Nachrichtendienste*, 1017).
- Dietrich, Jan-Hendrik*, Schriftliche Stellungnahme zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts“ (BT-Drucksache 19/26103) sowie zu weiteren Vorlagen der Fraktionen FDP und BÜNDNIS 90/DIE GRÜNEN (BT Drucksachen 19/19502, 19/19509 und 19/26221) v. 21.02.2021, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdrs. 19(4)731 G (zitiert: *Dietrich*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG).
- Dietrich, Jan-Hendrik*, Zusammenfassung und Anmerkung zu BVerfG, Urt. v. 19.5.2020 - 1 BvR 2835/17, *GSZ* 2020, 173–182 (zitiert: *Dietrich*, *GSZ* 2020).

- Donohue, Laura K.*, The Future of Foreign Intelligence, Privacy and Surveillance in a Digital Age, New York 2016.
- Dreier, Horst/Brosius-Gersdorf, Frauke* (Hrsg.), Grundgesetz Kommentar, Band I, Art. 1-19 Band III, Art. 83-146, 4. Aufl., 2023.
- Droste, Bernadette*, Handbuch des Verfassungsschutzrechts, Stuttgart u.a. 2007.
- Dürig, Günter et al.* (Hrsg.), Dürig/Herzog/Scholz, Grundgesetz Kommentar, 103. Aufl., München 2024.
- Durner, Wolfgang*, Anmerkung zu BVerfG, Urt v. 20.04.2016 — 1 BO 966/09, 1 BvIR 1140/09 — Verfassungswidrigkeit einzelner Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung, DVBl 2016, 780–784.
- Ehmann, Eugen/Selmayr, Martin* (Hrsg.), DSGVO Datenschutz-Grundverordnung, Kommentar, 3. Aufl., München 2024.
- Eichborn, Peter/Friedrich, Peter*, Verwaltungsökonomie I, Methodologie und Management der öffentlichen Verwaltung, Baden-Baden 1976.
- Eiffler, Sven-R.*, Exekutivkontrolle, Ministerielle Fachaufsicht und Koordinierung, in: Jan-Hendrik Dietrich, Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 1499–1532.
- Einsiedler, Mark*, Das richterliche Beratungsgeheimnis, NJ 2014, 6–13.
- Epping, Volker/Hillgruber, Christian* (Hrsg.), BeckOK Grundgesetz, 58. Edition, München 2024.
- European Data Protection Board*, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf; Stand: November 2020. Zuletzt abgerufen am: 31.08.2024.
- European Union Agency for Fundamental Rights*, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume II: field perspectives and legal update, 2017.
- Evers, Hans-Ulrich*, Parlamentarische Kontrolle der Nachrichtendienste, NJW 1978, 1144–1145.
- Fabrner, Matthias*, Unabhängige Gremien der ex ante-Rechtskontrolle - Ein Rat von Wächtern oder „Beischläfern“?, Zu den Rechten und Pflichten von Minderheiten und Einzelmitgliedern de lege lata et ferenda, GSZ 2023, 223–227.
- Friesenbahn, Ernst*, Die Kontrolle der Dienste, in: Bundesministerium des Innern (Hrsg.), Verfassungsschutz und Rechtsstaat, Köln u.a. 1981, S. 87–115.
- Gärditz, Klaus Ferdinand*, § 1 Auskunftersuchen gegenüber der Privatwirtschaft, in: Jan-Hendrik Dietrich, Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 967-1015 (zitiert: Gärditz, Hdb. des Rechts der Nachrichtendienste).
- Gärditz, Klaus Ferdinand*, Anmerkung zu BVerwG, Beschluss vom 29.4.2015 - 20 F 8.14 - Verweigerung der Vorlage von Geheimdienstakten, DVBl 2015, 903–910 (zitiert: Gärditz, DVBl 2015).
- Gärditz, Klaus Ferdinand*, Bundesnachrichtendienst semper reformanda, GSZ 2021, 905–914 (zitiert: Gärditz, GSZ 2021).
- Gärditz, Klaus Ferdinand*, Die Rechtsbindung des Bundesnachrichtendienstes bei Auslandstätigkeiten, Die Verwaltung 2015, 463–497 (zitiert: Gärditz, Die Verwaltung 2015).
- Gärditz, Klaus Ferdinand*, Die Reform des Nachrichtendienstrechts des Bundes: Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes und Stärkung des Parlamentarischen Kontrollgremiums, DVBl 2017, 525–534 (zitiert: Gärditz, DVBl 2017).

- Gärditz, Klaus Ferdinand*, Grundrechtliche Grenzen strategischer Ausland-Ausland-Telekommunikationsaufklärung, Ein Wegweiser durch die BND-Entscheidung des BVerfG, Urt. v. 19. 5. 2020 – 1 BvR 2835/17, JZ 2020, 825–835 (zitiert: *Gärditz*, JZ 2020).
- Gärditz, Klaus Ferdinand*, Konturen eines allgemeinen Nachrichtendienstverfassungsrechts 2022, <https://verfassungsblog.de/konturen-eines-allgemeinen-nachrichtendienstverfassungsrechts/>; Stand: Mai 2022. Zuletzt abgerufen am: 31.08.2024 (zitiert: *Gärditz*, Verfassungsblog vom 2.5.2022).
- Gärditz, Klaus Ferdinand*, Sicherheitsverfassungsrecht und technische Aufklärung durch die Nachrichtendienste, EuGRZ 2018, 6–22 (zitiert: *Gärditz*, EuGRZ 2018).
- Gärditz, Klaus Ferdinand*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts v. 16.02.2021, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdrs. 19(4)731 A (zitiert: *Gärditz*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG).
- Gärditz, Klaus Ferdinand*, Verfassungsschutzrecht und Datenübermittlung, Zugleich eine Besprechung von BVerfG, Urt. v. 26.4.2022 - 1 BvR 1619/17 = GSZ 2022, 137 ff., GSZ 2022, 161–170 (zitiert: *Gärditz*, GSZ 2022).
- Gazeas, Nikolaos*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, Berlin 2014.
- Geiger, Klaus*, Datenschutz bei den Verfassungsschutzbehörden, Vorschläge für eine Neukonzeption, DVBl 1990, 748–758.
- Golla, Sebastian*, Datenschutzrechtliche Schattengewächse in den Ländern, Herausforderungen bei der Umsetzung der JI-Richtlinie für die Polizei, KriPoZ 2019, 238–244.
- Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin* (Hrsg.), Das Recht der Europäischen Union, Band I EUV/AEUV, 81. Aufl., München 2024.
- Graulich, Kurt*, Befugnisse und Kontrolle des Bundesnachrichtendienstes bei der Fernmeldeaufklärung, GSZ 2021, 121–129 (zitiert: *Graulich*, GSZ 2021).
- Graulich, Kurt*, Justizgewährung und Geheimdienste, in: Kurt Graulich, Dieter Simon (Hrsg.), Terrorismus und Rechtsstaatlichkeit, Analysen, Handlungsoptionen, Perspektiven, Berlin 2007, S. 143–163 (zitiert: *Graulich*, Justizgewährung und Geheimdienste).
- Greenwald, Glen*, Die globale Überwachung, Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, München 2014 (zitiert: *Greenwald*, Globale Überwachung).
- Greenwald, Glen*, NSA collecting phone records of millions of Verizon customers daily, Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>; Stand: Juni 2013. Zuletzt abgerufen am: 31.08.2024 (*Greenwald*, NSA collecting phone records).
- Greis, Friedhelm*, G10-Kommission fühlt sich von BND dupliert, Operation Eikonal, <https://www.golem.de/news/operation-eikonal-g10-kommission-fuehlt-sich-von-bnd-duepiert-1503-113198.html>, Stand: März 2015. Zuletzt abgerufen am: 31.08.2024.
- Groeben, Hans von der/Schwarze, Jürgen/Hatje, Armin* (Hrsg.), Europäisches Unionsrecht, Vertrag über die Europäische Union Vertrag über die Arbeitsweise der Europäischen Union Charta der Grundrechte der Europäischen Union, 7. Aufl., Baden-Baden 2015.
- Gröpl, Christoph*, Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung, Legitimation, Organisation und Abgrenzungsfragen, Berlin 1993.

- Guber, Tillo*, Buchbesprechung v. Simon Kempny, Verwaltungskontrolle, DVBl 2019, 902–904.
- Gusy, Christoph*, Architektur und Rolle der Nachrichtendienste in Deutschland, ApuZ 2014, 9–14 (zitiert: *Gusy*, ApuZ 2014).
- Gusy, Christoph*, Beobachtung Organisierter Kriminalität durch den Verfassungsschutz?, StV 1995, 320–326 (zitiert: *Gusy*, StV 1995).
- Gusy, Christoph*, Das Trennungsprinzip zwischen Informationen von Nachrichtendiensten und Polizei, GSZ 2021, 142–149 (*Gusy*, GSZ 2021).
- Gusy, Christoph*, Der Schutz vor Überwachungsmaßnahmen nach dem Gesetz zur Beschränkung des Art. 10 GG, NJW 1981, 1581–1586 (*Gusy*, NJW 1981).
- Gusy, Christoph*, Grundrechte und Verfassungsschutz, Studien zur inneren Sicherheit 13, Wiesbaden 2011 (zitiert: *Gusy*, Grundrechte und Verfassungsschutz 2011).
- Gusy, Christoph*, Kontrolle der Nachrichtendienste, VerwArch 2015, 437–458 (zitiert: *Gusy*, VerwArch 2015).
- Gusy, Christoph*, Parlamentarische Kontrolle der Nachrichtendienste im demokratischen Rechtsstaat, ZRP 2008, 36–40 (zitiert: *Gusy*, ZRP 2008).
- Gusy, Christoph*, Polizei und Nachrichtendienste im Kampf gegen die Organisierte Kriminalität, KritV 1994, 242–251 (zitiert: *Gusy*, KritV 1994).
- Gusy, Christoph*, Rechtsgrundlagen der Richtervorbehalte nach § 100b StPO, GA 2003, 672–692.
- Gusy, Christoph*, Reformperspektiven des Rechts der Nachrichtendienste, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich et al. (Hrsg.), Reform der Nachrichtendienste, Tübingen 2019, S. 19–30 (zitiert: *Gusy*, Reformperspektiven).
- Gusy, Christoph*, Richterliche Kontrolle des Verfassungsschutzes, in: Bundesamt für Verfassungsschutz (Hrsg.), Verfassungsschutz in der Demokratie, 1990, S. 67–103 (zitiert: *Gusy*, Richterliche Kontrolle).
- Gusy, Christoph*, Verfassungsfragen vorbeugenden Rechtsschutzes, JZ 1998, 167–174 (zitiert: *Gusy*, JZ 1998).
- Häberle, Peter*, Die Abhörentscheidung des Bundesverfassungsgerichts vom 15.12.1970: Analyse und Kritik des Urts sowie des Minderheitsvotums vom 4. Januar 1971, JZ 1971, 145.
- Hahn, Caroline*, Die Aufsicht des öffentlich-rechtlichen Rundfunks, Bestandsaufnahme und Zukunftsperspektiven, Frankfurt 2010.
- Hanning, August/Schindler, Gerhard*, Ex-BND-Chefs nennen Nachrichtendienst „zahnlosen Wachhund“, Ein Gastbeitrag von den ehemaligen BND-Präsidenten August Hanning und Gehrhard Schindler, <https://www.bild.de/politik/inland/politik-inland/geheimdienst-nur-bedingt-einsatzbereit-ex-bnd-chefs-fordern-spionage-reform-84939156.bild.html>; Stand: August 2023. Zuletzt abgerufen am: 31.08.2024.
- Hansalek, Erik*, Die parlamentarische Kontrolle der Bundesregierung im Bereich der Nachrichtendienste, 2005.
- Hecker, Jan*, Allgemeine Verfassungsfragen der Nachrichtendienste, in: Jan-Hendrik Dietrich, Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 222–247.
- Heidebach, Martin*, Die NSA-Affäre in Deutschland - Stößt der Grundrechtsschutz an seine Grenzen?, DöV 2015, 594–599.
- Herzog, Roman*, Der Auftrag der Verfassungsschutzbehörden, in: Bundesministerium des Innern (Hrsg.), Verfassungsschutz und Rechtsstaat, Köln u.a. 1981, S. 1–18.
- Hetzer, Wolfgang*, Strafrechtspflege durch Geheimdienste?, StV 1999, 165–171.

- Hipp, Dietmar*, "Auswüchse beseitigen, an denen niemand Interesse haben kann", Interview mit Matthias Bäcker, <https://www.spiegel.de/panorama/justiz/auswuechse-beseitigen-an-denen-niemand-interesse-haben-kann-a-e5e28934-9f8a-4a5e-9065-5905f3f1bfb4>; Stand: April 2022. Zuletzt abgerufen am: 31.08.2024.
- Hirsch, Alexander*, Die Kontrolle der Nachrichtendienste, Vergleichende Bestandsaufnahme, Praxis und Reform, Berlin 1996.
- Hoch, Josef/Schmidt-Räntsch, Johanna/Brunst, Phillip*, Ein Jahr Rechtskontrolle der technischen Auslandsaufklärung des Bundesnachrichtendienstes, NVwZ 2023, 712–717.
- Hoch, Josef/Schmidt-Räntsch, Johanna/Tombrink, Christian/Weinland, Dietlind*, Diskussionsentwurf eines Gesetzes über den Unabhängigen Kontrollrat und zur Änderung des BND-Gesetzes, <https://ukrat.de/DE/UKRatG/UKRatG-Diskussionsentwurf.html?nn=15604>; Stand: August 2023. Zuletzt abgerufen am: 31.08.2024.
- Hoffmann-Riem, Wolfgang*, Tendenzen in der Verwaltungsrechtsentwicklung, DöV 1997, 433–442 (zitiert: *Hoffmann-Riem*, DöV 1997).
- Hoffmann-Riem, Wolfgang*, Verwaltungskontrolle- Perspektiven, in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann (Hrsg.), Verwaltungskontrolle, Baden-Baden 2001, S. 325–366 (zitiert: *Hoffmann-Riem*, Verwaltungskontrolle).
- Hong, Mathias*, Der Einsatz von V-Leuten und verdeckten Mitarbeitern zwischen sicherheitspolitischer Notwendigkeit und verfassungsrechtlichen Grenzen, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich et al. (Hrsg.), Reform der Nachrichtendienste, Tübingen 2019, S. 45–89.
- Huber, Bertold*, BND-Gesetzreform – gelungen oder nachbesserungsbedürftig?, ZRP 2016, 162–166 (zitiert: *Huber*, ZRP 2016).
- Huber, Bertold*, Das BVerfG und die Ausland-Ausland-Fernmeldeaufklärung des BND, NVwZ-Beilage 2020, 3–9 (zitiert: *Huber*, NVwZ-Beilage 2020).
- Huber, Bertold*, Geheime Überwachung von Mitarbeitern einer NGO ohne richterliche Genehmigung, NVwZ 2017, 1513–1514 (zitiert: *Huber*, NVwZ 2017).
- Huber, Bertold*, Kontrolle der Nachrichtendienste des Bundes- dargestellt am Beispiel der Tätigkeit der G 10-Kommission, GSZ 2017, 12-16 (zitiert: *Huber*, GSZ 2017).
- Huber, Bertold*, „Massenüberwachung“ vor dem EGMR, Die Entscheidungen in den Rechtssachen Big Brother Watch und Rättvisa, NVwZ-Beilage 2021, 3–10 (zitiert: *Huber*, NVwZ-Beilage 2013).
- Huber, Bertold*, Nachrichtendienste und EMRK – Die Spruchpraxis des EGMR zur Überwachung der Brief-, Post- und Telekommunikation durch Nachrichtendienste, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, Festgabe für Kurt Graulich zum 70. Geburtstag, Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik Bd. 3, Tübingen 2019, S. 191–205 (zitiert: *Huber*, Nachrichtendienste und EMRK).
- Huber, Bertold*, Post aus Pullach - Das G 10-Urt. des BVerfG vom 14.7.1999, NVwZ 2000, 393–396.
- Huber, Peter M./Voßkuhle, Andreas* (Hrsg.), Grundgesetz Kommentar, Band 1 Präambel Art. 1-19, 8. Aufl., München 2024 (zitiert: *Huber/Voßkuhle/Bearbeiter*).
- Hubert, Bert*, On my resignation as regulator of the Dutch intelligence and security services, <https://berthub.eu/articles/posts/resignation-as-intelligence-regulator/>; Stand: September 2022. Zuletzt abgerufen am: 31.08.2024.
- Huesmann, Felix*, Der Verfassungsschutz steht vor einer Reform, <https://www.rnd.de/politik/verfassungsschutz-in-bund-und-laendern-vor-umfassender-reform-BCACMYCMMJBUR-LUNG23OPNBDAU.html>; Stand: Juni 2022. Zuletzt abgerufen am: 31.08.2024.

- Jarass, Hans D.* (Hrsg.), Charta der Grundrechte der Europäischen Union, unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK, 4. Aufl., 2021.
- Johannes, Paul C./Weinhold, Robert*, Das neue Datenschutzrecht bei Polizei und Justiz, Europäisches Datenschutzrecht und deutsche Datenschutzgesetze, Baden-Baden 2018.
- Kahl, Wolfgang*, § 47 Begriff, Funktionen und Konzepte von Kontrolle, in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band III, Personal, Finanzen, Kontrolle, Sanktionen, Staatliche Einstandspflichten, 2. Aufl., München 2013, S. 459–592 (zitiert: *Kahl*, Kontrolle).
- Kahl, Wolfgang/Waldhoff, Christian/Walter, Christian* (Hrsg.), Bonner Kommentar Grundgesetz, 2023 (zitiert: *Kahl/Waldhoff/Walter-Bearbeiter*).
- Karpenstein, Ulrich/Mayer, Franz C.* (Hrsg.), Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Kommentar, 3. Aufl., München, Basel 2022 (zitiert: *Karpenstein/Mayer/Bearbeiter*).
- Karpenstein, Ulrich/Sangi, Roya*, Nationale Sicherheit im Unionsrecht: Zur Bedeutung von Art. 4 II 3 EUV, GSZ 2020, 162–168.
- Kauß, Udo*, Der suspendierte Datenschutz bei Polizei und Geheimdiensten, Frankfurt am Main, New York 1989.
- Kaysers, Hans Henning*, Die Unterrichtung Betroffener über Beschränkungen des Brief-, Post und Fernmeldegeheimnisses, Aktuelle Probleme des Artikel 10- Gesetzes und des Terrorismusbekämpfungsgesetzes, AöR 2004, 121–140.
- Kempny, Simon*, Verwaltungskontrolle, Zur Systematisierung der Mittel zur Sicherung administrativer Rationalität unter besonderer Berücksichtigung der Gerichte und der Rechnungshöfe, Tübingen 2017.
- Knaust, Maik*, Matrix einer neuen Generation auslandsnachrichtendienstlicher Überwachungstätigkeit, Das Recht der inneren und äußeren Sicherheit Band 20, Berlin 2022.
- Kornblum, Thorsten*, Rechtsschutz gegen geheimdienstliche Aktivitäten, Berlin 2011.
- Krebs, Walter*, Kontrolle in staatlichen Entscheidungsprozessen, Ein Beitrag zur rechtlichen Analyse von gerichtlichen, parlamentarischen und Rechnungshof-Kontrollen, Heidelberg 1984.
- Kugelmann, Dieter*, Datenschutz bei Polizei und Justiz, Der Richtlinienvorschlag der Kommission, DuD 2012, 581–583.
- Kühling, Jürgen/Buchner, Benedikt* (Hrsg.), Datenschutz- Grundverordnung, BDSG Kommentar, 4. Aufl., München 2024.
- Kutscha, Martin*, Rechtsschutzdefizite bei Grundrechtseingriffen von Sicherheitsbehörden, NVwZ 2003, 1296–1300.
- Lachenmann, Matthias*, Das Ende des Rechtsstaats aufgrund der digitalen Überwachung durch die Geheimdienste?, DöV 2016, 501–511.
- Lampe, Klaus von*, Bekämpfung der Organisierten Kriminalität, in: Jan-Hendrik Dietrich, Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, 781-816.
- Leigh, Ian/Wegge, Njord*, Intelligence oversight at the outset of the twenty-first century, in: Ian Leigh, Njord Wegge (Hrsg.), Intelligence Oversight in the twenty-first century, Accountability in a changing world, Abingdon, New York 2019, S. 7–24.
- Leyendecker, Hans/Pinkert, Reiko*, BND behindert Kontrollgremium bei der Arbeit, <https://www.sueddeutsche.de/politik/exklusiv-bnd-behindert-kontrollgremium-bei-der-arbeit-1.3782566>; Stand: Dezember 2017. Zuletzt abgerufen am: 31.08.2024.
- Liesching, Marc* (Hrsg.), BeckOK Jugendschutzrecht, 2. Aufl., München.

- Lindner, Josef Franz/Unterreitmeier, Johannes*, Grundlagen einer Dogmatik des Nachrichtendienstrechts, DöV 2019, 165–175.
- Linzbach, Karoline Maria/Gärditz, Klaus Ferdinand*, Das nachrichtendienstliche Trennungsgebot- ein verfassungsrechtlicher Totenschein, ZG 2020, 314–355.
- Löffelmann, Markus*, Der Schutz grundrechtssensibler Bereiche im Sicherheitsrecht, GSZ 2019, 190–196 (zitiert: *Löffelmann*, GSZ 2019).
- Löffelmann, Markus*, Die Zukunft der deutschen Sicherheitsarchitektur - Vorbild Bayern?, GSZ 2018, 85–91 (zitiert: *Löffelmann*, GSZ 2018).
- Löffelmann, Markus*, Schriftliche Stellungnahme zur öffentlichen Anhörung am 18. Februar 2021 zu BT-Drs. 19/26103, 19/26221, 19/19502 und 19/509 v. 18.02.2021, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschuss-Drs. 19(4)731 C (zitiert: *Löffelmann*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG).
- Löffelmann, Markus*, Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz, Berlin 2022 (zitiert: *Löffelmann*, Überwachungsgesamtrechnung).
- Löffelmann, Markus*, VI § 3 Heimliche Ton- und Bildaufzeichnungen, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 1093–1158 (zitiert: *Löffelmann*, Hdb. des Rechts der Nachrichtendienste).
- Löffelmann, Markus*, VI § 4 Überwachung des Brief-, Post- und Fernmeldeverkehrs, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 1159–1282 (zitiert: *Löffelmann*, Hdb. des Rechts der Nachrichtendienste, S. 1159).
- Löffelmann, Markus*, VI § 5 Sonstige Telekommunikationsüberwachung, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, 1283–1343 (zitiert: *Löffelmann*, Hdb. des Rechts der Nachrichtendienste, S. 1283).
- Löffelmann, Markus/Zöller, Mark A.*, Nachrichtendienstrecht, Baden-Baden 2022 (zitiert: *Löffelmann/Zöller*, Nachrichtendienstrecht).
- Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian* (Hrsg.), Grundgesetz, Band 1, Präambel, Art. 1–19, 4. Aufl., München 1999.
- Markard, Nora*, Stellungnahme Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts (BT-Drucksache 19/26103), Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschuss-Drs. 19(4)731 D (zitiert: *Markard*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG).
- Marsch, Nikolaus*, Das europäische Datenschutzgrundrecht, Grundlagen- Dimensionen- Verflechtungen, Tübingen 2018.
- Marxsen, Christian*, Strategische Fernmeldeaufklärung, Neuerungen in den Kompetenzen des Bundesnachrichtendienstes, DöV 2018, 218–229.
- Masing, Johannes*, Nachrichtendienste im freiheitlichen Rechtsstaat, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich et al. (Hrsg.), Nachrichtendienste im demokratischen Rechtsstaat, Tübingen 2018, S. 3–19.
- Meinel, Florian*, Stellungnahme zur Anhörung des Innenausschusses des Deutschen Bundestages zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts (BNDG-E, BT-Drucksache 19/26103) sowie weiterer Gesetzentwürfe und Anträge v. 18.02.2021, Deutscher Bundestag, Ausschuss für Inneres und Heimat Ausschuss-Drs. 19(4)731 B.

- Meyer-Ladewig, Jens/Raumer, Stefan von/Nettesheim, Martin* (Hrsg.), EMRK, 5. Aufl., Baden-Baden, Wien, Basel 2023.
- Michel, Anna*, Parlamentarische Kontrolle des Verfassungsschutzes in Bund und Ländern, GSZ 2021, 197–203 (zitiert als: *Michel*, GSZ 2021, 197).
- Michel, Anna*, Zur Reform der Verfassungsschutzkontrolle: Waurm die Reformpläne der Bundesregierung begrüßenswert sind und dennoch ausgeweitet werden müssen, <https://verfassungsblog.de/zur-reform-der-verfassungsschutzkontrolle/>, Stand: Juli 2022. Zuletzt abgerufen am: 31.08.2024 (zitiert als *Michel*, Verfassungsblog vom 18.7.2022).
- Möllers, Christoph*, Von der Kernbereichsgarantie zur exekutiven Notstandsprärogative: zum BND-Sektoren-Beschluss des BVerfG, Besprechung von BVerfG. Beschluss v. 13.10.2016 - 2 BvE 2/15, JZ 2017, 271–278.
- Monroy, Matthias*, Geheimdienste auf Abwegen, In einem europäischen Netzwerk arbeiten Behörden seit sieben Jahren weitgehend unkontrolliert, <https://www.nd-aktuell.de/artikel/1170972-geheimdienstkontrolle-geheimdienste-auf-abwegen.html>; Stand: Februar 2023. Zuletzt abgerufen am: 31.08.2024.
- Möstl, Markus/Schwabenbauer, Thomas* (Hrsg.), BeckOK Polizei- und Sicherheitsrecht Bayern, 20. Aufl., München 2022.
- Muckel, Stefan*, Fernmeldeaufklärung im Ausland im BND-Gesetz verfassungswidrig geregelt, JA 2020, 631–635.
- Muižnieks, Nils*, Bericht des Menschenrechtskommissars des Europarats nach seinem Besuch in Deutschland, <https://rm.coe.int/09000016806db804>; Stand: Oktober 2015. Zuletzt abgerufen am: 31.08.2024.
- Müller, Michael/Schwabenbauer, Thomas*, Vorgaben des Unionsrechts und der Europäischen Menschenrechtskonvention, in: Hans Liskén, Erhard Denninger, Matthias Bäcker et al. (Hrsg.), Handbuch des Polizeirechts, 7. Auflage, München 2021, S. 952–1008.
- Müller-Terpitz, Ralf*, Die »strategische Kontrolle« des internationalen Telekommunikationsverkehrs durch den Bundesnachrichtendienst, Jura 2000, 296–302.
- Münch, Ingo von/Kunig, Philip* (Hrsg.), Grundgesetz-Kommentar: GG, Band 1: Präambel bis Art. 69, 7. Aufl., München 2021.
- Nehm, Kay*, Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur, NJW 2004, 3289–3295.
- Ní Loideain, Nóra*, EU Data Privacy Law and Serious Crime, Data retention and policymaking, 2019.
- Nolte, Martin*, Kontrolle als zentrales Element unseres Verfassungsstaats, in: Kontrolle im verfassten Rechtsstaat, Kieler Dokumentation des 50. Wissenschaftlichen Werkstattgesprächs am 10. August 2002 in Kiel anlässlich des 60. Geburtstag von Albert von Mutius, Kiel 2002, S. 11–31.
- Notz, Konstantin von*, Die Rolle der Nachrichtendienste in der Extremismusbekämpfung, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich et al. (Hrsg.), Radikalisierung und Extremismus, Aufgabenfelder und Herausforderungen der Nachrichtendienste, Tübingen 2023, S. 113–118.
- Ogorek, Markus*, Leitlinien für den Verfassungsschutzverbund, NJW 2022, 1570–1573.
- Paeffgen, Hans-Ullrich*, Das Urt. des Bundesverfassungsgerichts zum G 10 in der Fassung des Verbrechensbekämpfungsgesetzes 1994, StV 1999, 668–678.
- Petri, Thomas*, § 20 Grundrechtlicher Datenschutz und sicherheitsbehördliche Überwachung, in: Jan-Hendrik Dietrich, Matthias Fahrner, Nikolaos Gazeas et al. (Hrsg.), Handbuch Sicherheits- und

- Staatsschutzrecht, München 2022, S. 667–715 (zitiert: *Petri*, Hdb. Sicherheits- und Staatsschutzrecht).
- Petri, Thomas*, Déjà vu – datenschutzpolitische Aufarbeitung der PRISM-Affäre Appell nach mehr Transparenz der nachrichtendienstlichen Tätigkeit, ZD 2013, 557–561 (zitiert: *Petri*, ZD 2013).
- Petri, Thomas*, Erfolgreiche Verfassungsbeschwerde gegen Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz in ihrer derzeitigen Form, Anmerkung, ZD 2020, 409–412 (zitiert: *Petri*, ZD 2020).
- Peuker, Enrico*, Unionsrechtliche Regelungskompetenzen im Bereich der nationalen Sicherheit. Zur Auslegung von Art. 4 Abs. 2 S. 3 EUV unter kritischer Würdigung der EuGH-Rechtsprechung, EuR 2023, 535–563.
- Pfeiffer, Kristin*, Wie europäisch wird deutsches Polizeirecht?, Wie über das Datenschutzrecht die Europäisierung des Polizeirechts betrieben wird 2021, <https://verfassungsblog.de/wie-europaisch-wird-deutsches-polizeirecht/>; Stand: April 2021. Zuletzt abgerufen am: 31.08.2024.
- Pfeiffer, Thomas*, Radikalisierungsprävention durch Verfassungsschutz, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich et al. (Hrsg.), Radikalisierung und Extremismus, Aufgabenfelder und Herausforderungen der Nachrichtendienste, Tübingen 2023, S. 173–183.
- Poscher, Ralf/Kappler, Katrin*, Staatstrojaner für Nachrichtendienste: Zur Einführung der Quellen-Telekommunikationsüberwachung im Artikel 10-Gesetz, <https://verfassungsblog.de/staatstrojaner-nachrichtendienste/>; Stand: Juli 2021. Zuletzt abgerufen am: 31.08.2024.
- Poscher, Ralf/Kilchling, Michael/Landerer, Lukas*, Überwachungsbarometer für Deutschland, Ein Modellkonzept, https://shop.freiheit.org/download/P2@1168/542535/Analyse_Ueberwachung_Teil2_260122_final.pdf; Stand: Januar 2022. Zuletzt abgerufen am: 31.08.2024.
- Poscher, Ralf/Rusteberg, Benjamin*, Die Aufgabe des Verfassungsschutzes, Zur funktionalen Trennung von Polizei und Nachrichtendiensten, KJ 2014, 57–71.
- Riegel, Reinhard*, Die Kontrolle von Überwachungsmaßnahmen nach dem Gesetz zu Art. 10 GG, Die Kontrollzuständigkeit der Datenschutzbeauftragten, DöV 1985 (zitiert *Riegel*, DöV 1985).
- Riegel, Reinhard*, Zur Novellierungsbedürftigkeit des Gesetzes zu Art. 10 GG, ZRP 20 (1987), 431–436.
- Riegel, Reinhard* (Hrsg.), Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10), München 1997 (zitiert: *Riegel/Bearbeiter*).
- Rieger, Thomas*, Nachrichtendienst und Rechtsstaat, ZRP 1985, 3–11.
- Roggan, Fredrik* (Hrsg.), G-10-Gesetz, 2. Aufl., 2018.
- Ruckerbauer, Corbinian*, Die Stärkung des Datenschutzbeauftragten als Schlüssel zu einer effektiveren Nachrichtendienstkontrolle, <https://www.stiftung-nv.de/sites/default/files/snv-impuls-staerkung-des-bfdi-fuer-eine-effektivere-nachrichtendienstkontrolle.pdf>; Stand: März 2024. Zuletzt abgerufen am: 31.08.2024.
- Rusche-meier, Hannah*, Der additive Grundrechtseingriff, Berlin 2019.
- Rüß, Oliver*, Internationale nachrichtendienstliche Zusammenarbeit, in: Jan-Hendrik Dietrich, Sven-R. Eißler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 458–505.
- Sachs, Michael*, Verfassungsrechtliche Determinanten der öffentlichen Verwaltung in Deutschland, Juridica International 21 (2014), 58, <https://ojs.utlib.ee/index.php/juridica/article/view/JI.2014.21.05> (zitiert: *Sachs*, Juridica International 21 (2014)); Stand: November 2014. Zuletzt abgerufen am: 31.08.2024.
- Sachs, Michael* (Hrsg.), Grundgesetz Kommentar, 9. Aufl., München 2021 (zitiert: *Sachs/Bearbeiter*).

- Sajfert, Juraj/Quintel, Teresa*, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, SSRN Journal 2017, 1–22.
- Schenke, Wolf-Rüdiger*, Polizei- und Ordnungsrecht, Heidelberg 2018 (zitiert: *Schenke*, Polizei- und Ordnungsrecht).
- Schenke, Wolf-Rüdiger/Graulich, Kurt/Ruthig, Josef*, Sicherheitsrecht des Bundes, München 2019 (zitiert: *Schenke/Graulich/Ruthig-Bearbeiter*).
- Scheuner, Ulrich*, Verantwortung und Kontrolle in der demokratischen Verfassungsordnung, in: Theo Ritterspach (Hrsg.), Festschrift für Gebhard Gebhard Müller, 1970, S. 379–402.
- Schlink, Bernhard*, Das Abhörurteil des Bundesverfassungsgerichts, Der Staat 1973, 85–108.
- Schmahl, Stefanie*, Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste?, JZ 2014, 220–228.
- Schmidt-Aßmann, Eberhard*, Das allgemeine Verwaltungsrecht als Ordnungsidee, Grundlagen und Aufgaben der verwaltungsrechtlichen Systembildung, 2. Aufl., Berlin, Heidelberg 2006 (zitiert: *Schmidt-Aßmann*, Ordnungsidee).
- Schmidt-Aßmann, Eberhard*, Verwaltungskontrolle, -Einleitende Problemskizze-, in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann (Hrsg.), Verwaltungskontrolle, Baden-Baden 2001, S. 9–45 (zitiert: *Schmidt-Aßmann*, Verwaltungskontrolle).
- Schmidt-Räntsch, Johanna*, Der neue unabhängige Kontrollrat, K&R 2022, 34–41.
- Schmitt, Betram/Köhler, Marcus* (Hrsg.), Meyer-Goßner/Schmitt Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 63. Aufl., München 2020.
- Schneider, Bastian*, Fernmeldegeheimnis und Fernmeldeaufklärung, Berlin 2020.
- Schneider, Franziska*, Kernbereich privater Lebensgestaltung, JuS 2021, 29–34 (zitiert: *Schneider*, JuS 2021).
- Schneider, Franziska*, Wen genau beobachtet eigentlich der Verfassungsschutz?, ZD 2021, 360–365 (zitiert: *Schneider*, ZD 2021).
- Scholz, Rupert/Pitschas, Rainer*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984.
- Schönfeldt, Kristina*, Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, Tagungsbericht zum 2. Symposium zum Recht der Nachrichtendienste, JZ 2018, 927–929.
- Schulze, Kira/Bange, Mirko*, Die (fehlenden) Abhilfebefugnisse des BfDI nach § 16 Abs. 2 BDSG, Europarechtskonforme Umsetzung oder rechtswidrige Gesetzeslücke?, ZD 2019, 199–204.
- Schütz, Philip*, Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich, in: Alexander Roßnagel, Michael Friedewald, Marit Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes, DuD-Fachbeiträge, Wiesbaden 2018, S. 251–268.
- Schwabenbauer, Thomas*, Heimliche Grundrechtseingriffe, Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Tübingen 2013 (zitiert: *Schwabenbauer*, Heimliche Grundrechtseingriffe).
- Schwabenbauer, Thomas*, Informationsverarbeitung im Polizei- und Strafverfahrensrecht (G), Teil 1., in: Erhard Denninger, Matthias Bäcker, Kurt Graulich (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr- Strafverfolgung - Rechtsschutz, 7. Aufl., Köln 2021, S. 842–952 (zitiert: *Schwabenbauer*, Hdb. des Polizeirechts).
- Schwander, Timo*, Extraterritoriale Wirkung von Grundrechten im Mehrebenensystem, Berlin 2019.

- Schwarze, Jürgen et al.* (Hrsg.), EU-Kommentar, 4. Aufl., Baden-Baden 2019.
- Stiems, Thomas*, Folgewirkungen des BVerfG-Urteils zum BKAG bei den Sicherheitsbehörden - eine erste Bilanz, NWVbl 2018, 1-7.
- Singer, Jens* (Hrsg.), Praxiskommentar zum Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, Kontrollgremiumgesetz - PKGrG, Berlin, Heidelberg 2016.
- Sobr, Karsten/Kemmerich, Thomas*, Kapitel 3. Technische Grundlagen der Informationssicherheit, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, Rechtshandbuch, 2. Aufl., München 2023, S. 49-115.
- Sosna, Sabine*, Der BfDI – ein Kontrollorgan unter dem Radar?, Datenschutzaufsicht über die Nachrichtendienste des Bundes, GSZ 2022, 245-251.
- Spindler, Gerald/Schuster, Fabian* (Hrsg.), Recht der elektronischen Medien, 4. Aufl., München 2019.
- Steiner, Elisabeth*, „Big Brother Watch/Centrum för Rättvisa“, Die strategische Fernmeldeaufklärung des Bundesnachrichtendienstes im Spiegel der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte, GSZ 2024, 32-38 (zitiert: *Steiner*, GSZ 2024).
- Steiner, Elisabeth*, Zur Leistungsfähigkeit der gerichtsähnlichen Vorabkontrolle der technischen Auslandsaufklärung des Bundesnachrichtendienstes, GSZ 2023, 124-130 (zitiert: *Steiner*, GSZ 2023).
- Steinke, Ronen*, Die dunklen Geheimdienstfürsten 21.10.2016, <https://www.sueddeutsche.de/politik/bnd-die-dunklen-geheimdienstfuersten-1.3216355> (zitiert als: Die dunklen Geheimdienstfürsten); Stand: Oktober 2016. Zuletzt abgerufen am: 31.08.2024 (zitiert: *Steinke*, Die dunklen Geheimdienstfürsten).
- Steinke, Ronen*, Früherer BND-Chef kritisiert Kontrollsystem des deutschen Geheimdiensts 22. 9. 2016, <https://www.sueddeutsche.de/politik/bundesnachrichtendienst-angriff-auf-die-lauscher-1.3174459> (zitiert als: Früherer BND-Chef kritisiert Kontrollsystem des deutschen Geheimdiensts); Stand: September 2016. Zuletzt abgerufen am: 31.08.2024 (zitiert: *Steinke*, Früherer BND-Chef kritisiert Kontrollsystem des deutschen Geheimdiensts).
- Steinke, Ronen*, Verfassungsschutz, Wie der Geheimdienst Politik macht, Berlin, München 2023 (zitiert: *Steinke*, Verfassungsschutz).
- Steinke, Ronen*, Wie die Bundesregierung den Verfassungsschutz einhegen will, <https://www.sueddeutsche.de/politik/verfassungsschutz-reform-bundesregierung-karlsruhe-1.5605167?reduced=true> (zitiert als: *Steinke*, Wie die Bundesregierung den Verfassungsschutz einhegen will); Stand: Juni 2022. Zuletzt abgerufen am: 31.08.2024 (zitiert: *Steinke*, Wie die Bundesregierung den Verfassungsschutz einhegen will).
- Stevens, Jeremy/Limberger, Victor*, Der primärrechtliche Rahmen für die Abgrenzung von DSGVO und JI-Richtlinie, JZ 2022, 656-663.
- Stoklas, Jonathan/Wendorf, Joris*, BND-Prüfbericht der BfDI: Haben wir ein Kontrolldefizit?, ZD-Aktuell 2016, 5345.
- Strößenreuther, Martin*, Die behördeninterne Kontrolle, 1991.
- Sule, Satish*, National Security and EU law restraints on Intelligence Activities, in: Jan-Hendrik Dietrich, Satish Sule (Hrsg.), Intelligence law and policies in Europe, A handbook, München, Oxford, Baden-Baden 2019, S. 335-387.
- Taege, Jürgen/Gabel, Detlev* (Hrsg.), DSGVO- BDSG- TTDSG, Kommentar, 4. Aufl., Frankfurt am Main 2022.

- Talmon, Stefan*, Der Begriff der "Hoheitsgewalt" in Zeiten der Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste, JZ 2014, 783–787.
- Tanneberger, Steffen*, Die Sicherheitsverfassung, Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts, zugleich ein Beitrag zu einer induktiven Methodenlehre, Tübingen 2014.
- Thomé, Sarah*, Reform der Datenschutzaufsicht, Effektiver Datenschutz durch verselbstständigte Aufsichtsbehörden, Wiesbaden 2015.
- Tombrink, Christian*, Der Unabhängige Kontrollrat – ein Teil der Justiz?, GSZ 2024, 28–32.
- Unterreitmeier, Johannes*, Das informationelle Trennungsprinzip – eine historisch-kritische Relecture, AöR 2019, 234–298 (zitiert: *Unterreitmeier*, AöR 2019).
- Unterreitmeier, Johannes*, Überwachung durch Polizei oder Nachrichtendienst – kein Unterschied?, GSZ 2018, 1–6 (zitiert: *Unterreitmeier*, GSZ 2018).
- Venedig-Kommission*, Report on the Democratic Oversight of the Security Services, Juni 2007 (zitiert als: *Venedig-Kommission*, Report 2007).
- Venedig-Kommission*, Report of the democratic oversight of the security services 2015 (zitiert als: *Venedig-Kommission*, Report 2015).
- Vogt, Jannis*, Novellierte strategische Ausland-Fernmeldeaufklärung im Bundesnachrichtendienstgesetz, Neue Normen, alte Probleme?, DöV 2023, 689–698 (zitiert: *Vogt*, DöV 2023).
- Vogt, Jannis*, Strategische Auslandstelekommunikationsüberwachung durch den Bundesnachrichtendienst, Berlin 2023 (zitiert: *Vogt*, Strategische Auslandstelekommunikationsüberwachung).
- Waldhoff, Christian*, Die reformierte Kontrolle der Nachrichtendienste durch das Parlamentarische Kontrollgremium und das Unabhängige Gremium, in: Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich et al. (Hrsg.), Reform der Nachrichtendienste, Tübingen 2019, S. 73–89.
- Warg, Gunter*, § 12 Betroffene Personen im personellen Geheimschutz, in: Jan-Hendrik Dietrich, Matthias Fahrner, Nikolaos Gazeas et al. (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, München 2022, S. 381–424 (zitiert: *Warg*, Hdb. Sicherheits- und Staatsschutzrecht).
- Warg, Gunter*, Der gesetzliche Auftrag der deutschen Nachrichtendienste, in: Jan-Hendrik Dietrich, Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, S. 509–581 (zitiert: *Warg*, Hdb. des Rechts der Nachrichtendienste).
- Warg, Gunter*, Kapitel 18. Nachrichtendienstrecht, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, Rechtshandbuch, 2. Aufl., München 2023, S. 797–848 (zitiert: *Warg*, Nachrichtendienstrecht).
- Warg, Gunter*, Recht der Nachrichtendienste, Stuttgart 2023 (zitiert: *Warg*, Recht der Nachrichtendienste).
- Watt, Eliza*, The legacy of the privacy versus security narrative in the ECtHR's jurisprudence, 21.4.2021, <https://verfassungsblog.de/os6-privacy-vs-security/> Stand: April 2021. Zuletzt abgerufen am: 31.08.2024.
- Weinhold, Robert/Johannes, Paul C.*, Europäischer Datenschutz in Strafverfolgung und Gefahrenabwehr – Die neue Datenschutz-Richtlinie im Bereich Polizei und Justiz sowie deren Konsequenzen für deutsche Gesetzgebung und Praxis, DVBl 2016, 1501–1506.
- Weisser, Niclas-Frederic*, Der Richtervorbehalt im Nachrichtendienstrecht, DöV 2014, 831–836.
- Werthebach, Eckart/Droste-Lehnen, Bernadette*, Organisierte Kriminalität, ZRP 1994, 57–65.

- Wetzling, Thorsten*, Bedingt kontrollfähig: Warum der Unabhängige Kontrollrat einer Reform bedarf, https://www.stiftung-nv.de/sites/default/files/snv_impuls_warum-der-unabhaengige-kontrollrat-einer-reform-bedarf.pdf; Stand: Februar 2024. Zuletzt abgerufen am: 31.08.2024 (zitiert als: *Wetzling*, Bedingt kontrollfähig).
- Wetzling, Thorsten*, Die Nachrichtendienstkontrolle muss modernisiert werden 2020, <https://netzpolitik.org/2020/die-nachrichtendienstkontrolle-muss-modernisiert-werden/>; Stand: Januar 2020. Zuletzt abgerufen am: 31.08.2024 (zitiert als: *Wetzling*, Nachrichtendienstkontrolle).
- Wetzling, Thorsten*, Entmystifiziert die Spione, Gastkommentar Geheimdienstkontrolle 25.11.2018, <https://taz.de/Gastkommentar-Geheimdienstkontrolle/!5549796/>; Stand: November 2018. Zuletzt abgerufen am: 31.08.2024 (zitiert als: *Wetzling*, Gastkommentar).
- Wetzling, Thorsten*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes v. 21.2.2021, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschuss-Drs. 19(4)731 F (zitiert: *Wetzling*, Stellungnahme Entwurf eines Gesetzes zur Änderung des BNDG).
- Wetzling, Thorsten/Dietrich, Charlotte*, Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?, <https://www.interface-eu.org/publications/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier>; Stand: November 2022. Zuletzt abgerufen am: 31.08.2024.
- Wetzling, Thorsten/Moßbrucker, Daniel*, BND-Reform, die Zweite, Vorschläge zur Neustrukturierung der Nachrichtendienst-Kontrolle, https://www.interface-eu.org/storage/archive/files/bnd_reform_die_zweite_vorschlaege_zur_neustrukturierung.pdf; Stand: Juni 2020. Zuletzt abgerufen am: 31.08.2024.
- Wetzling, Thorsten/Ruckerbauer, Corbinian*, Zügellose Überwachung?, Defizite der Kontrolle des Militärischen Nachrichtenwesens der Bundeswehr, <https://www.interface-eu.org/publications/defizite-der-kontrolle-des-militaerischen-nachrichtenwesens-der-bundeswehr>; Stand: Oktober 2023. Zuletzt abgerufen am: 31.08.2024 (zitiert als: *Wetzling/Ruckerbauer*, Zügellose Überwachung?).
- Wetzling, Thorsten/Vieth, Kilian*, Datenbasierte Nachrichtendienstkontrolle, Agenda für mehr Wirksamkeit, 2020, https://www.stiftung-nv.de/sites/default/files/datenbasierte_nachrichtendienstkontrolle.pdf; Stand: Mai 2020. Zuletzt abgerufen am: 31.08.2024 (zitiert als: *Wetzling/Vieth*, Datenbasierte Nachrichtendienstkontrolle).
- Wetzling, Thorsten/Vieth, Kilian*, Massenüberwachung bändigen, Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich, Schriften zur Demokratie, <https://www.interface-eu.org/archive/publications/2537>; Stand: März 2019. Zuletzt abgerufen am: 31.08.2024 (zitiert als: *Wetzling/Vieth*, Massenüberwachung bändigen).
- Wetzling, Thorsten/Vieth, Kilian*, Mehr Rechtskontrolle wagen, Warum das Mandat des Unabhängigen Kontrollrats erweitert werden sollte, <https://www.interface-eu.org/publications/3500>; Stand: Juni 2023. Zuletzt abgerufen am: 31.08.2024 (zitiert als: *Wetzling/Vieth*, Mehr Rechtskontrolle wagen).
- Wills, Aidan/Born, Hans*, International intelligence cooperation and accountability, Formidable challenges and imperfect solutions, in: Hans Born, Ian Leigh, Aidan Wills (Hrsg.), International Intelligence Cooperation and Accountability, New York 2011, 277-308.
- Winter, Felicia*, Rahmenbedingungen für eine Kohärenz des Nachrichtendienstrechts, Baden-Baden 2022.

- Wissenschaftliche Dienste Deutscher Bundestag*, Überwachungsgesamtrechnung, Abgrenzung zum additiven Grundrechtseingriff, <https://www.bundestag.de/resource/blob/889448/6c895218de75aa0a1617841f913aa85c/WD-3-017-22-pdf-data.pdf>, Stand: Februar 2022. Zuletzt abgerufen am: 31.08.2024.
- Wöckel, Holger*, Justizielle Kontrolle, insb. Rechtsschutz gegen nachrichtendienstliche Aktivitäten, in: Jan-Hendrik Dietrich, Sven-R. Eiffler (Hrsg.), *Handbuch des Rechts der Nachrichtendienste*, Stuttgart 2017, S. 1607–1654.
- Wolff, Heinrich Amadeus*, Verfassung in ausgewählten Teilrechtsordnungen: Konstitutionalisierung und Gegenbewegungen- Sicherheitsrecht, DVBl 2015, 1076–1084 (zitiert *Wolff*, DVBl 2015).
- Wolff, Heinrich Amadeus*, Vorratsdatenspeicherung – Der Gesetzgeber gefangen zwischen Europarecht und Verfassung?, NVwZ 2010, 751–753 (zitiert: *Wolff*, NVwZ 2010).
- Wolff, Heinrich Amadeus/Brink, Stefan* (Hrsg.), *BeckOK Datenschutzrecht, DS-GVO, BDSG, Grundlagen, Bereichsspezifischer Datenschutz*, 48. Aufl., München (zitiert: *Wolff/Brink/Bearbeiter*).
- Zalnieriute, Monika*, A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union, *Modern Law Review* 2022, 198–218 (zitiert: *Zalnieriute*, *Modern Law Review* 2022).
- Zalnieriute, Monika*, Big Brother Watch and others v. the United Kingdom. App Nos. 58170/13, 62322/14, 24960/15. Judgement. European Court of Human Rights (Grand Chamber), May 25, 2021, *American Journal of International Law* 2022, 585–592 (zitiert: *Zalnieriute*, *American Journal of International Law* 2022).
- Zalnieriute, Monika*, Big Brother Watch v. UK: Procedural Fetishism and Mass Surveillance under the ECHR, 2.6.2021, <https://verfassungsblog.de/big-b-v-uk/>, Stand: Juni 2021. Zuletzt abgerufen am: 31.08.2024 (zitiert: *Zalnieriute*, *Verfassungsblog* vom 2.6.2021).
- Zöller, Mark A.*, Der Rechtsrahmen der Nachrichtendienste bei der „Bekämpfung“ des internationalen Terrorismus, JZ 2007, 763–771.
- Zöllner, Dieter*, *Der Datenschutzbeauftragte im Verfassungssystem, Grundsatzfragen der Datenschutzkontrolle*, Berlin 1995.

Anna Höning (geb. Michel)

Externe Rechtskontrolle der Nachrichtendienste

Nach den jüngsten Entscheidungen des Bundesverfassungsgerichts muss die externe Rechtskontrolle der Nachrichtendienste grundlegend überarbeitet werden. In diesem Buch wird dargelegt, welche höherrangigen Vorgaben dafür gelten, wie die Kontrolle in Bund und Ländern ausgestaltet ist und wie sich die herausgearbeiteten Defizite beheben ließen.