Institut für Gesetzesfolgenabschätzung und Evaluation

Evaluation nach Artikel 5 Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismus-bekämpfungsgesetzen vom 3. Dezember 2015

Im Auftrag des
Bundesministeriums des Innern, für Bau und Heimat
Berlin

Projektleiter:
Prof. Dr. Jan Ziekow

Projektbearbeiter:
Axel Piesker, M.A.
Tim Vallée, Ass. iur., LLM., M.A.

Juli 2018

Inhaltsverzeichnis

Abbildungsverzeichnis **5**

Tabellenverzeichnis **6**

Abkürzungsverzeichnis **8**

1. Einleitung **10**

2. Evaluationsauftrag und -umfang **11**

3. Methodisches Vorgehen **13**

4. Empirische und rechtswissenschaftliche Analyse der Anwendungspraxis der zu evaluierenden Regelungen **17**

4.1. § 3 Abs. 1 Nr. 4 BVerfSchG, § 5 Abs. 2 BVerfSchG, § 1 Abs. 1 S. 2 MADG (mit Folgeänderung in § 18 Abs. 1 BVerfSchG) 17

4.1.1. Genese der Regelungen 17

4.1.2. Empirische Ergebnisse 17

4.1.3. Rechtswissenschaftliche Bewertung 19

4.2. § 8a-c BVerfSchG, § 3 BNDG, § 4a MADG 20

4.2.1. Genese der Regelungen 20

4.2.2. Empirische Ergebnisse 28

4.2.2.1. Überblick 28

4.2.2.2. § 8a Abs. 1 BVerfSchG, § 3 BNDG und § 4a MADG (Bestandsdatenauskunft bei Telediensteanbietern) 32

4.2.2.3. § 8a Abs. 2 und 2a BVerfSchG, § 3 BNDG und § 4a MADG 33

4.2.2.4. Bewertung und Optimierungsbedarf aus Sicht der Nachrichtendienste 47

4.2.3. Rechtswissenschaftliche Bewertung 51

4.2.3.1. § 8a BVerfSchG 51

4.2.3.2. § 8b BVerfSchG 52

4.3. § 9 Abs. 4 BVerfSchG, § 5 BNDG, § 5 MADG 53

4.3.1. Genese der Regelungen 53

4.3.2. Empirische Ergebnisse 53

4.3.3. Rechtswissenschaftliche Bewertung 61

4.4. § 12 Abs. 3 BVerfSchG, § 20 Abs. 1 BNDG, § 6 Abs. 2 MADG 63

4.4.1. Genese der Regelungen 63

4.4.2. Empirische Ergebnisse 63

4.4.3. Rechtswissenschaftliche Bewertung 66

4.5. § 17 Abs. 3 BVerfSchG 66

4.5.1. Genese der Regelung 66

4.5.2. Empirische Ergebnisse 67

4.5.3. Rechtswissenschaftliche Bewertung 75

4.6. § 18 Abs. 1a BVerfSchG 76
4.6.1. Genese der Regelungen 76
4.6.2. Empirische Ergebnisse 76
4.6.3. Rechtswissenschaftliche Bewertung 83
4.7. § 19 Abs. 4 und 5 BVerfSchG, § 11 Abs. 1 S. 1 MADG 84
4.7.1. Genese der Regelungen 84
4.7.2. Empirische Ergebnisse 85
4.7.3. Rechtswissenschaftliche Bewertung 85
4.8. § 10 Abs. 1 und 3 MADG 86
4.8.1. Genese der Regelung 86
4.8.2. Empirische Ergebnisse 86
4.8.3. Rechtswissenschaftliche Bewertung 86
4.9. § 11 Abs. 1 S. 3 MADG 87
4.9.1. Genese der Regelung 87
4.9.2. Empirische Ergebnisse 87
4.9.3 Rechtswissenschaftliche Bewertung 87
4.10. § 24 Abs. 1 und 2 BNDG 88
4.10.1. Genese der Regelung 88
4.10.2. Empirische Ergebnisse 88
4.10.3. Rechtswissenschaftliche Bewertung 89
4.11. § 1 Abs. 4 und 5 SÜG 89
4.11.1. Genese der Regelung 89
4.11.2. Empirische Ergebnisse 91
4.11.2.1. Statistische Ergebnisse und Einschätzungen der betroffenen Behörden ... 92
4.11.2.1.1. Nichtöffentlicher und öffentlicher Bereich 92
4.11.2.1.2. Militärischer Sicherheitsbereich 102
4.11.2.2. Zentrale Ergebnisse der Befragung der Sabotageschutz- bzw. Sicherheitsbeauftragten im öffentlichen, nichtöffentlichen und militärischen (Sicherheits-)Bereich 106
4.11.2.2.1. Nichtöffentlicher Bereich 106
4.11.2.2.2. Öffentlicher Bereich 119
4.11.2.2.3. Militärischer Sicherheitsbereich 124
4.11.2.3. Gegenüberstellung der zentralen empirischen Ergebnisse für den nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich 131
4.11.3. Rechtswissenschaftliche Bewertung 135

5. Probleme der Anwendungspraxis im Spiegel der Konsistenz nachrichtendienstlicher Befugnisse 138
5.1. Zentrale Ergebnisse 138
5.2. Verfassungsrechtlicher und sicherheitspolitischer Rahmen 138
5.3. Überlegungen zu den einzelnen Befugnissen 139
5.3.1. § 8 Abs. 1 BVerfSchG (Bestandsdaten Teledienste) 139
5.3.2. § 8a Abs. 2 S. 1 Nr. 1 BVerfSchG (Flugdaten) 140
5.3.3. § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG (Finanztransferdaten) 141
5.3.4. § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG (TK-Verkehrsdaten) sowie § 8a Abs. 2 S. 1 Nr. 5 BVerfSchG (Nutzungsdaten Telediensteanbieter) 141
5.3.5. § 8a Abs. 2a BVerfSchG (Kontostammdaten) 141
5.3.6. § 9 Abs. 4 BVerfSchG (IMSI-Catcher) 142
5.3.7. § 8a Abs. 2 S. 1 Nr. 3 a. F. BVerfSchG (Postdienstleister) 143
6. Fallstudienanalyse 145
7. Zusammenfassung der Ergebnisse 147
8. Literaturverzeichnis 154
9. Anhang 156
9.1. Konkrete Fallbeispiele für den Einsatz der Maßnahmen nach § 8a Abs. 2 und 2a BVerfSchG 156
9.1.1. Fallbeispiele zu § 8a Abs. 2 S. 1 Nr. 2 und Abs. 2a BVerfSchG 156
9.1.2. Fallbeispiele zu § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG 157
9.2. Konkrete Fallbeispiele für den Einsatz des IMSI-Catchers 158
9.3. Anhang begleitende Erhebung 160
9.3.1. Begründung für die Nutzenbewertung (BfV, BAMAD und BND) (§ 8a Abs. 2 und 2a BVerfSchG, § 3 BNDG und § 4a MADG) 160
9.3.2. Begründung für die Nutzenbewertung (BfV und BAMAD) (§ 17 Abs. 3 BVerfSchG) 163
9.3.3. Begründung für die Nutzenbewertung (§ 18 Abs. 1a BVerfSchG) (nur Länder) 176

Abbildungsverzeichnis

Abb. 1: Anordnungen nach Phänomenbereichen 36

Abb. 2: Bewertung des konkreten Nutzens der gewonnenen Informationen für die nachrichtendienstliche Arbeit 41

Abb. 3: Bewertung der Reaktionszeit der nach § 8 Abs. 2 S. 1 Nr. 1 und 4 BVerfSchG zur Auskunft verpflichteten Unternehmen durch BfV und BAMAD 42

Abb. 4: Bewertung der Reaktionszeit der nach § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG zur Auskunft verpflichteten Unternehmen sowie des BZSt durch BfV, BND und BAMAD 43

Abb. 5: Bewertung des Nutzens der mittels IMSI-Catcher gewonnenen Informationen durch das BfV und BAMAD 57

Abb. 6: SIS II-Ausschreibungen nach Phänomenbereichen 72

Abb. 7: Bewertung der im Rahmen der SIS II-Ausschreibung gewonnenen Informationen für die nachrichtendienstliche Arbeit 73

Abb. 8: Spontanübermittlungen der Ausländer- an die Landesverfassungsschutzbehörden 80

Abb. 9: Umgang mit den von den Ausländerbehörden übermittelten Informationen 81

Abb. 10: Bewertung des Nutzens der gemäß § 18 Abs. 1a BVerfSchG übermittelten Informationen für die nachrichtendienstliche Arbeit 82

Abb. 11: Anteil der Unternehmen nach Unternehmensart 107

Abb. 12: Unternehmensgröße der Fremdfirmen 109

Abb. 13: Größe der Unternehmen mit eigener sicherheitsempfindlicher Stelle 111

Abb. 14: Anwendungsbereiche der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) 114

Abb. 15: Verteilung der Sabotageschutzbeauftragten nach Behördentypen 119

Abb. 16: Bewertung der zeitlich erweiterten Ausnahmereglung (§ 9 Abs. 2 Nr. 2 SÜG) 121

Abb. 17: Bewertung des mit der Umsetzung des vpS verbundenen Aufwands durch die Sabotageschutzbeauftragten im öffentlichen Bereich 122

Abb. 18: Bewertung der vom BfV übermittelten Informationen (Votum) durch die Sabotageschutzbeauftragten im öffentlichen Bereich 123

Abb. 19: Bewertung der Zusammenarbeit mit dem BfV durch die Sabotageschutzbeauftragten im öffentlichen Bereich 123

Abb. 20: Anzahl der SiBe nach Organisationsbereichen 125

Abb. 21: Anwendungsbereiche der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) im militärischen Sicherheitsbereich 127

Abb. 22: Bewertung der zeitlich erweiterten Ausnahmereglung (§ 9 Abs. 2 Nr. 2 SÜG) durch die SiBe 128

Abb. 23: Bewertung der Zusammenarbeit mit dem BAMAD durch die SiBe 130

Tabellenverzeichnis

Tab. 1: Anzahl der Anordnungen nach § 8a Abs. 1, 2 und 2a BVerfSchG 29

Tab. 2: Art der Datenerhebungsmaßnahme nach Unternehmenstypen 29

Tab. 3: Anzahl der Anordnungen der besonderen Auskunftsverlangen gemäß § 8a Abs. 2 BVerfSchG nach Nachrichtendiensten 2002-2015.....31

Tab. 4: Anordnungen gemäß § 8a Abs. 2 und Abs. 2a BVerfSchG nach Nachrichtendiensten.....33

Tab. 5: Gründe für die Datenerhebung gemäß § 8a Abs. 2 und 2a BVerfSchG.....34

Tab. 6: Anzahl und Art der Personen, gegen die sich die Anordnung gemäß § 8a Abs. 2 und 2a BVerfSchG richtete 37

Tab. 7: Informationen, die gemäß § 8a Abs. 2 und 2a BVerfSchG erhoben wurden 38

Tab. 8: Gründe für den Einsatz des IMSI-Catcher 55

Tab. 9: Begründungen des BfV und BAMAD für die Nutzenbewertung der mittels IMSI-Catcher gewonnenen Informationen.....58

Tab. 10: Anzahl der SIS-Ausschreibungen (1.10.2016-30.9.2017) 68

Tab. 11: Gründe für die Ausschreibung im SIS II.....68

Tab. 12: Treffermeldungen im SIS II.....69

Tab. 13: Übermittlungen der SIS II-Informationen nach Ländern 70

Tab. 14: Art der bei den Zufallskontrollen übermittelten Informationen 71

Tab. 15: Anzahl der Übermittlungen gemäß § 18 Abs. 1a BVerfSchG nach Abteilungen des BfV.....78

Tab. 16: Anzahl der Speicherungen nach Abteilungen des BfV (absolut und in %) 78

Tab. 17: SÜ im nichtöffentlichen Bereich 2015-2017 95

Tab. 18: SÜ im öffentlichen Bereich 2015-2017 97

Tab. 19: SÜ im militärischen Sicherheitsbereich 2015-2017.....105

Tab. 20: Art der Unternehmen, in welche die Fremdfirmen Personal entsenden, nach SÜFV-Typisierung 108

Tab. 21: Art der Unternehmen mit eigener sicherheitsempfindlicher Stelle nach SÜFV-Typisierung.....110

Tab. 22: Art der Unternehmen, für die die Aufgabe des Sabotageschutzbeauftragten wahrgenommen wird 112

Tab. 23: Bewertung der Relevanz der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich 115

Tab. 24: Bewertung der zeitlichen erweiterten Ausnahmeregelung als ausreichend durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich 115

Tab. 25: Anwendung der Anerkennensregelung (§ 2 Abs. 1 S. 5 SÜG) durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich.....116

Tab. 26: Bewertung des mit der Umsetzung des vpS in den Unternehmen verbundenen Aufwands durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich 118

Tab. 27: Bewertung der Zusammenarbeit mit dem BMWi durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich....118

Tab. 28: Eingruppierung der für den vpS relevanten Akteure im militärischen Sicherheitsbereich....125

Tab. 29: Bewertung des mit der Umsetzung des vpS in den Dienststellen verbundenen Aufwands im militärischen Sicherheitsbereich 129

Tab. 30: Eingeleitete und abgeschlossene SÜ vpS im nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich 132

Tab. 31: Bewertung der Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) im nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich 133

Tab. 32: Nutzung der Anerkennensregelung (§ 2 Abs. 1 S. 5 SÜG) im nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich 134

Tab. 33: Bewertung des mit der Umsetzung des vpS verbundenen Aufwands im nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich 135

Abkürzungsverzeichnis

ABH	Ausländerbehörde
AZR	Ausländerzentralregister
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BAMF	Bundesamt für Migration und Flüchtlinge
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BKamt	Bundeskanzleramt
BImA	Bundesanstalt für Immobilienaufgaben
BMI	Bundesministerium des Innern, für Bau und Heimat
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BVerfG	Bundesverfassungsgericht
BZR	Bundeszentralregister
BZSt	Bundeszentralamt für Steuern
DA-Sicherheit	Dienstanweisung Sicherheit (BAMF)
DA-Asyl	Dienstanweisung Asyl (BAMF)
GB	Geheimschutzbeauftragte/r
GG	Grundgesetz
IMSI	International Mobile Subscriber Identity
IS	Islamischer Staat
LfV	Landesverfassungsschutzbehörde
LKA/LKÄ	Landeskriminalamt/Landeskriminalämter
HöSi	Höherer Offizier Absicherung
NADIS WN	Nachrichtendienstliches Informationssystem Wissensnetz
PKK	Arbeiterpartei Kurdistans (Partiya Karkerên Kurdistanê)
PNR	Passenger Name Record
seS	sicherheitsempfindliche Stelle
seT	sicherheitsempfindliche Tätigkeit
SiBe	Sicherheitsbeauftragte/r

SIS II	Schengener Informationssystem II
SÜ	Sicherheitsüberprüfung
TK	Telekommunikation
TKÜ	Telekommunikationsüberwachung
vpS	vorbeugender personeller Sabotageschutz
VS	Verschlusssache
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

1. Einleitung

In Deutschland existieren auf Bundesebene mit dem Bundesamt für Verfassungsschutz (BfV), dem Bundesnachrichtendienst (BND) sowie dem Bundesamt für den Militärischen Abschirmdienst (BAMAD) drei Nachrichtendienste, deren Hauptaufgabe in der Sammlung und Auswertung von Informationen besteht. Das Nachrichtendienstrecht wurde im Laufe der Jahrzehnte immer weiter kodifiziert. Das erste Gesetz zum Verfassungsschutz erließ das Parlament im Jahre 1950. Die knapp gefassten fünf Paragrafen wurden den Anforderungen an das Recht auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht (BVerfG) im Jahre 1983 bestimmt hatte, nicht mehr gerecht. Im Jahre 1990 erfolgten daher eine Novellierung sowie die erste parlamentsgesetzliche Regelung für den MAD und den BND. Durch die Anschläge des 11. September 2001 entstand eine neue Sicherheitslage, die den Deutschen Bundestag seitdem zu insgesamt drei großen Novellierungen des Rechts der Nachrichtendienste in den Jahren 2002, 2007 und 2011 veranlasste.

Während sich das sog. erste Anti-Terrorpaket der straf- und vereinsrechtlichen Bekämpfung des Terrorismus widmete, enthielt das zweite Anti-Terrorpaket das Terrorismusbekämpfungsgesetz (im Folgenden kurz: TBG; beide 2002). Im Jahre 2007 erfolgte eine Erweiterung der Bestimmungen zur Bekämpfung des Terrorismus mit dem sog. Terrorismusbekämpfungsergänzungsgesetz (im Folgenden kurz: TBEG). Eine weitere Novellierung nahm der Gesetzgeber im Jahre 2011 mit dem Gesetz zur Änderung des Bundesverfassungsschutzgesetzes vor (im Folgenden kurz: Änderungsgesetz).

Die mit dem TBG geänderten Bestimmungen im Bundesverfassungsschutzgesetz (BVerfSchG), MAD-Gesetz (MADG), BND-Gesetz (BNDG) und Sicherheitsüberprüfungsgesetz (SÜG) waren zunächst bis zum 10. Januar 2007 befristet, während das TBEG die einheitliche Befristung aufhob und im Einzelnen diejenigen Normen benannte, die einer Verlängerung unterlagen. Insoweit verlängerte sich die Befristung auf den 9. Januar 2012. Das Änderungsgesetz aus dem Jahr 2011 verlängerte die Geltungsdauer der Regelungen bis zum 9. Januar 2016. Auf Grundlage der im April 2015 abgeschlossenen Evaluation[1] wurde am 3. Dezember 2015 das Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen, das eine erneute Befristung und Evaluation der Befugnisse zur Auskunftseinholung bei u. a. Luftfahrtunternehmen, Kreditinstituten, Telekommunikationsdiensten und Telediensten sowie der Vorschriften zur Einführung des vorbeugenden personellen Sabotageschutzes vorsah, vom Deutschen Bundestag verabschiedet.[2] Sofern der Bundestag diese Bestimmungen nicht verlängert, wird am 10. Januar 2021 die Rechtslage vom 31. Dezember 2001 wiederhergestellt.

[1] Vgl. Bundesregierung, BT-Drs. 18/5935.
[2] Vgl. Gnüchtel, NVwZ 2016, 13 (13).

2. Evaluationsauftrag und -umfang

Artikel 5 des Gesetzes zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen vom 3. Dezember 2015 sieht vor, dass die Anwendung der durch das TBG, das TBEG, das Änderungsgesetz aus dem Jahr 2011 und dieses Gesetz geschaffenen und geänderten Vorschriften des BVerfSchG, des MADG, des BNDG und des SÜG von der Bundesregierung vor dem 10. Januar 2021 unter Einbeziehung eines wissenschaftlichen Sachverständigen oder mehrerer wissenschaftlicher Sachverständiger, die im Einvernehmen mit dem Deutschen Bundestag bestellt werden, evaluiert werden. Bei der Untersuchung sind auch die Häufigkeit und die Auswirkungen der mit den Eingriffsbefugnissen verbundenen Grundrechtseingriffe einzubeziehen und in Beziehung zu setzen zu der anhand von Tatsachen darzustellenden Wirksamkeit zum Zweck der Terrorismusbekämpfung.

Gemäß der Leistungsbeschreibung sollen dabei folgende Regelungen näher untersucht werden:

(1) BVerfSchG

- § 3 Abs. 1 Nr. 4 BVerfSchG (Zuständigkeit der Verfassungsschutzbehörden für die Aufklärung von Bestrebungen gegen den Gedanken der Völkerverständigung usw.),
- § 3 Abs. 2 S. 2 BVerfSchG (Konkretisierung der Aufgaben der Verfassungsschutzbehörden),
- § 5 Abs. 2 BVerfSchG (Konkretisierung der Zuständigkeitsabgrenzung der Verfassungsschutzbehörden durch Verweis auf § 3 Abs. 1 BVerfSchG),
- §§ 8a bis 8c BVerfSchG (besondere Auskunftsverlangen),
- § 9 Abs. 4 BVerfSchG (IMSI-Catcher),
- § 12 Abs. 3 Satz 2 BVerfSchG (Angleichung der Löschungsfrist auf 10 Jahre in bestimmten Fällen),
- § 17 Abs. 3 BVerfSchG (Ausschreibung auf Veranlassung der Nachrichtendienste im Schengener Informationssystem),
- § 18 Abs. 1 BVerfSchG (Konkretisierung der für die Übermittlung von Informationen an das BfV relevanten Schutzgüter),
- § 18 Abs. 1a BVerfSchG (Spontanübermittlungen durch das Bundesamt für Migration und Flüchtlinge (BAMF) bzw. Ausländerbehörden an Verfassungsschutzbehörden) sowie
- § 19 Abs.4 und 5 BVerfSchG (Datenübermittlung durch Verfassungsschutzbehörden auch zur Gewährleistung der Sicherheit von lebens- und verteidigungswichtigen Einrichtungen; Mitteilung an Betroffene; keine Anwendung bei Datenerhebung).

(2) MADG

- § 1 Abs. 1 S. 2 MADG (Zuständigkeit des MAD zur Aufklärung von Bestrebungen gegen den Gedanken der Völkerverständigung usw.),
- § 1 Abs. 3 MADG (Klarstellung der Mitwirkung des MAD an Sicherheitsüberprüfungen des vorbeugenden personellen Sabotageschutzes),
- § 4a MADG (besondere Auskunftsverlangen),

- § 5 MADG (Einsatz IMSI-Catcher),
- § 10 Abs. 1 und 3 MADG (Übermittlung von Informationen an den MAD und Einsichtnahme in amtliche Register im Zusammenhang mit Bestrebungen gegen den Gedanken der Völkerverständigung),
- § 11 Abs. 1 S. 1 MADG (Übermittlungen nach § 19 Abs. 4 in Verbindung mit Abs. 5 BVerfSchG (an Private)) sowie
- § 11 Abs. 1 S. 3 MADG (Weiterübermittlung von Spontanübermittlungen des BAMF).

(3) BNDG[3]

- § 3 BNDG (besondere Auskunftsverlagen),
- § 5 BNDG (Einsatz IMSI-Catcher)
- § 20 Abs. 1 BNDG (zehnjährige Prüffrist) sowie
- § 24 Abs. 2 BNDG (Übermittlungsbefugnisse des BND entsprechend der erweiterten Regelungen nach dem BVerfSchG).

(4) SÜG

- § 1 Abs. 4 und 5 SÜG (Sicherheitsüberprüfungen im Bereich des vorbeugenden personellen Sabotageschutzes)
- § 9 Abs. 2 Nr. 2 SÜG (Verlängerung des Zeitraums für die Beschäftigung an einer sicherheitsempfindlichen Stelle ohne SÜ) sowie
- weitere im SÜG und in Verordnungen anwendbare Bestimmungen zum vorbeugenden personellen Sabotageschutz.

Die Evaluation konzentriert sich darauf, die Neuerungen, die sich durch die letzte gesetzliche Änderung ergeben haben, einer vertieften Analyse zu unterziehen.
Ausweislich des erteilten Auftrags wird die Evaluation nicht durch den beauftragten wissenschaftlichen Sachverständigen, sondern durch die Bundesregierung durchgeführt. Der Sachverständige unterstützt die Bundesregierung durch Sicherstellung der Einhaltung wissenschaftlich-methodischer Standards. Dabei bezieht sich die Begutachtung allein auf die Beschreibung und wissenschaftliche Bewertung der Folgen, die sich aus der Anwendung der zu evaluierenden Vorschriften ergeben. Die empirisch ermittelten Grundrechtseingriffe sind zur Wirksamkeit zum Zwecke der Terrorismusbekämpfung dadurch in Beziehung zu setzen, dass die Anwendungspraxis juristisch, insbesondere hinsichtlich der Geeignetheit und Erforderlichkeit der Eingriffe, zu bewerten ist. Bei der Abwägung der Angemessenheit ist zu beachten, dass die politische Bewertung der in der begleitenden Begutachtung erzielten Ergebnisse nicht Bestandteil des Gutachtenauftrags ist. Ebenso wenig ist der Gutachter beauftragt worden, eine allgemeine verfassungsrechtliche Bewertung der zu evaluierenden Normen vorzunehmen oder zur Sicherheitsarchitektur im Übrigen oder eventuellen weiteren technischen Möglichkeiten Stellung zu nehmen.

[3] Die hier genannten §§ beziehen sich auf die umfangreiche Novellierung im Jahr 2017.

3. Methodisches Vorgehen

Auf Basis der Leistungsbeschreibung wurden in einem ersten Schritt die Prüfkriterien festgelegt, anhand derer die näher zu untersuchenden Regelungen bewertet wurden. Folgende Prüfkriterien wurden für die Datenerhebung im Rahmen des Evaluationsvorhabens ausgewählt und weiter operationalisiert:

(1) Eingriffsbreite

- Zahl der Eingriffe,
- Anzahl der Betroffenen sowie
- Menge der erhobenen Daten.

(2) Eingriffstiefe

- Art und Umfang der personenbezogenen Daten,
- Weiterverwendung der personenbezogenen Daten sowie
- Eingriffsdauer.

(3) Praktikabilität der Neuregelungen/der erweiterten Zuständigkeiten

- Anwendungserfahrungen/-praxis der Nachrichtendienste,
- Anwendungserfahrungen/-praxis der betroffenen Unternehmen sowie
- mögliche Anwendungsprobleme.

(4) Aufwand im Zusammenhang mit den besonderen Auskunftsverlangen für die Unternehmen

- Personalkosten für die Bearbeitung der Auskunftsverlangen,
- Zeitaufwand für die Bearbeitung der Auskunftsverlangen sowie
- sonstige Kosten, die im Zusammenhang mit der Bearbeitung der Auskunftsverlangen entstanden sind.

(5) Nicht-intendierte Effekte und mögliche Anwendungsprobleme

- Erfassung negativer Auswirkungen der Auskunftsverlangen auf die Hauptbetroffenen sowie
- Erfassung sonstiger nicht-intendierter Effekte.

(6) Wirksamkeit zum Zweck der Terrorismusbekämpfung

- Bewertung des Nutzens der gewonnenen Informationen für die Arbeit der Nachrichtendienste sowie
- Alternativen zur Ausübung der relevanten Befugnis.

In einem nächsten Schritt wurde das Erhebungsinstrumentarium entwickelt, um die für die Evaluation benötigten Daten gewinnen zu können. Neben der Auswertung der Berichte des Parlamentarischen Kontrollgremiums (PKGr) über die Anwendung der Regelungen durch die Nachrichtendienste war es erforderlich, eine **begleitende Erhebung** von Anwendungsfällen durchzuführen, die am 1. Oktober 2016 begann und am 30. September 2017 endete. Es wurden insgesamt drei Erhebungszeiträume festgelegt (1. Oktober bis 30. November 2016,

1. Dezember 2016 bis 30. April 2017 und 1. Mai bis 30. September 2017), um bereits erste Daten zur Vorbereitung der noch zu führenden qualitativen Interviews nutzen zu können. Eine retrospektive Datenerhebung mittels der vom Institut für Gesetzesfolgenabschätzung und Evaluation (InGFA) erarbeiteten Erhebungsinstrumente für den Zeitraum 1. Dezember 2014 bis 30. September 2015 war nach Angaben der Nachrichtendienste nicht/nur teilweise möglich bzw. wäre nur mit erheblichem Aufwand möglich gewesen, sodass darauf in Absprache mit dem Auftraggeber verzichtet wurde.
Die begleitende Datenerhebung diente in erster Linie dazu, im Vergleich zu den für den Bundestag erstellten vorhandenen Statistiken weitere – vor allem quantitative – Daten erfassen zu können. Je nach Regelung erfolgte eine Einzelfallerhebung – so wurden z. B. bei den besonderen Auskunftsverlangen einzelne Anordnungen erfasst – oder eine aggregierte Erfassung aller Anwendungsfälle für die oben genannten Zeiträume (z. B. § 1 Abs. 1 S. 2 MADG). Die erste Datenerhebungsphase (1. Oktober bis 30. November 2016) wurde zudem genutzt, um die für die jeweiligen Regelungen entwickelten Erhebungsbögen einem Praxistest zu unterziehen. Dieser führte jedoch zu keinen Veränderungen am Erhebungsinstrumentarium. Aufgrund nicht vorhersehbarer Entwicklungen musste allerdings bei einigen Vorschriften das Vorgehen bei der Datenerhebung angepasst werden. So war die Anzahl der gemäß § 8a Abs. 1 BVerfSchG durchgeführten Maßnahmen deutlich höher als bei der vorherigen Evaluation. Dies führte dazu, dass aufgrund der hohen Anzahl nicht für jede einzelne Maßnahme ein Erhebungsbogen ausgefüllt wurde, sondern die Daten vom BfV aggregiert übermittelt wurden. Dies hatte zur Folge, dass keine einzelfallbezogene Bewertung der von den zur Auskunft verpflichteten Unternehmen übermittelten Informationen seitens des BfV vorgenommen werden konnte. Zudem war es nicht möglich, die von den Unternehmen ans BfV übermittelten Daten einzelfallbezogen zu erfassen. Für eine Darstellung des Gesamtbildes hat dies jedoch keine Auswirkungen.
Ein ähnliches Problem ergab sich im Evaluationszeitraum bei den Spontanübermittlungen vom BAMF an das BfV. Auch hier war gegenüber der vorherigen Evaluation ein signifikanter Anstieg der Spontanübermittlungen feststellbar, der dazu führte, dass nicht jede einzelne Übermittlung des BfV mittels des von InGFA entwickelten Erhebungsbogens erfasst werden konnte. Stattdessen wurden auch hier mittels des Nachrichtendienstlichen Informationssystems (NADIS WN) die erforderlichen Daten aggregiert erfasst und an das InGFA übermittelt. Dadurch war es jedoch für das BfV nicht möglich, für jede Übermittlung des BAMF einzelfallbezogene Angaben (z. B. zur Art der gespeicherten personenbezogenen Daten oder zum Erkenntniswert der einzelnen vom BAMF übermittelten Informationen) zu machen.
Zusätzlich zur begleitenden Erhebung wurden **leitfadengestützte Experteninterviews** durchgeführt. Diese dienten zum einen dazu, Informationen zur Anwendungspraxis der Regelungen zu gewinnen, für die die Nutzung eines Erhebungsbogens in Absprache mit dem Auftraggeber als nicht sinnvoll erachtet wurde. Zum anderen konnten mit ihrer Hilfe zu den Regelungen, zu denen bereits Daten erhoben wurden, zusätzliche – vor allem qualitative – Daten zu den Anwendungserfahrungen gewonnen werden. Hierzu wurden im September 2017 vom InGFA Interviewleitfäden erarbeitet und die entsprechenden Interviewpartnerinnen und -partner identifiziert. Zwischen Oktober und Dezember 2017 wurden mit Vertreterinnen und Vertretern des BMI, des BMVg, des BMWi, des BAMF sowie der drei Nachrichtendienste leitfadengestützte Interviews geführt.
Die Arbeit der Nachrichtendienste ist durch komplexe und vielschichtige Verfahren der Informationsgewinnung geprägt. Dabei geht es u. a. darum, rechtzeitig Indikatoren zu identifizieren, die terroristisches Handeln vorbereiten oder begünstigen können. Darüber hinaus zielt die

nachrichtendienstliche Beobachtung darauf ab, die infrastrukturelle Basis der Beobachtungsobjekte (Organisationsstrukturen, Personengeflechte, Finanzströme und Reisewege) aufzuklären, um damit zur Entwicklung von Gegenmaßnahmen beizutragen. Neben der aktiven Extremismusbekämpfung geht es auch um die Früherkennung, um künftige, sich möglicherweise verstärkende Gefahren prognostizieren zu können. Die Nachrichtendienste verfügen aufgrund des Trennungsgebots nicht über Zwangsmittel zur Durchsetzung von Maßnahmen.
Empirisch lässt sich die Wirksamkeit der zu evaluierenden Maßnahmen nur schwer anhand von „Erfolgskriterien" (z. B. Zahl der eingeleiteten Strafverfahren oder Verurteilungen) messen, da sich diese nicht aus dem Aufgabenspektrum der Nachrichtendienste ableiten lassen. Vorrangig vermag daher eine Operationalisierung des Wirksamkeitskriteriums über eine Bewertung durch die Nachrichtendienste wertvolle Hinweise für die Bewertung einer Norm zu liefern. Darüber hinaus ermöglichen zusätzliche Informationen zu ausgewählten Fallbeispielen, die im Erhebungszeitraum vom BfV zur Verfügung gestellt wurden, einen besseren Einblick, wie die mit Hilfe der Maßnahmen gemäß § 8a Abs. 2 und 2a BVerfSchG und § 9 Abs. 4 BVerfSchG gewonnenen Informationen genutzt wurden (siehe Anhang, S. 156 ff.). Eine weitergehende Wirksamkeitserfassung bedürfte einer beobachtenden Begleitung der nachrichtendienstlichen Arbeit über einen längeren Zeitraum. In Anbetracht des damit verbundenen Personalaufwandes und der Kenntniserlangung von höchststufigen Geheimhaltungsgraden unterliegenden Informationen ist ein solcher Zugang weder Gegenstand des erteilten Auftrags noch konnte er innerhalb des vorgesehenen Evaluierungszeitraums zur Verfügung gestellt werden.
Darüber hinaus war es erforderlich, die durch die besonderen Auskunftsverlangen (§§ 8a-c BVerfSchG, § 3 BNDG sowie § 4a MADG) betroffenen Unternehmen in die Evaluation einzubeziehen. Im Rahmen der begleitenden Erhebung bei den Nachrichtendiensten wurde den zur Auskunft verpflichteten Unternehmen direkt bei der Abfrage ein Informationsschreiben mit einem Fragebogen-Link zur Verfügung gestellt. Der damit verknüpfte Kurzfragebogen konnte dann von den betroffenen Unternehmen am Computer ausgefüllt werden. Da lediglich eine grobe Zuordnung (z. B. Kreditinstitut, Luftfahrtunternehmen) erfolgte und keine Unternehmens- und Personennamen angegeben werden mussten, war die Anonymität der Unternehmen bei der Beantwortung der Fragebögen gewährleistet. Da sich allerdings bis Januar 2018 kein einziges Unternehmen an der Befragung beteiligt hatte, verzichtete das InGFA nach Rücksprache mit dem Auftraggeber darauf, die zur Auskunft verpflichteten Unternehmen auf anderem Weg anzusprechen.
Eine Neuerung gegenüber der vorherigen Evaluation stellte die **Befragung der Sabotageschutz- (öffentlicher und nichtöffentlicher Bereich) bzw. Sicherheitsbeauftragten (militärischer Sicherheitsbereich)** dar. Hierzu wurden vom InGFA in enger Abstimmung mit dem BMI, BMVg und BMWi standardisierte Fragebögen entwickelt, die über das jeweils zuständige Ministerium an die Sabotageschutz- bzw. Sicherheitsbeauftragten weitergeleitet wurden. Für den öffentlichen und nichtöffentlichen Bereich wurden die passwortgeschützten Fragebögen mittels LimeSurvey erstellt. Im nichtöffentlichen Bereich wurden in enger Abstimmung mit dem BMWi drei „Unternehmenstypen"[4] identifiziert, für die spezifische Fragen entwickelt wurden. Das BMWi verschickte das Begleitschreiben mit Fragebogen-Link und Passwort Ende April 2017 postalisch an alle dort registrierten Unternehmen. Für den öffent-

[4] Zu nennen sind hier (1) Unternehmen mit eigener sicherheitsempfindlicher Stelle mit eigenem Sabotageschutzbeauftragten, (2) Fremdfirmen mit eigenem Sicherheitsbeauftragten und (3) sog. „Sabotageschutz-Dienstleister", welche die Funktion des Sabotageschutzbeauftragten für andere Unternehmen wahrnehmen.

lichen Bereich wurde das BMI gebeten, das Begleitschreiben mit Fragebogen-Link und Passwort an die obersten Bundesbehörden zu schicken, die dieses dann Anfang Mai 2017 an die nachgeordneten Behörden in ihrem Geschäftsbereich weiterleiteten. Den Sabotageschutzbeauftragten aus dem öffentlichen und nichtöffentlichen Bereich wurde zunächst eine Frist von vier Wochen (bis Anfang Juni 2017) für die Beantwortung des Fragebogens gesetzt. Anfang Juni 2017 wurde vom BMI und BMWi noch einmal eine Erinnerungsnachricht verschickt, in der die Behörden bzw. Unternehmen, die bislang noch nicht an der Befragung teilgenommen hatten, gebeten wurden, den Fragebogen innerhalb von zwei Wochen auszufüllen. Im militärischen Sicherheitsbereich wurden die Fragebögen Mitte August 2017 vom BMVg als Word-Formulare an die Höheren Offiziere Absicherung, die Geheimschutzbeauftragten sowie ausgewählte Sicherheitsbeauftragte verschickt. Für die Beantwortung der Fragebögen wurde eine Frist von vier Wochen eingeräumt. Die Rückläufer wurden vom BMVg gesammelt und dann per E-Mail an das InGFA geschickt. Diese drei Personengruppen wurden nach Rücksprache mit dem BMVg in die Untersuchung einbezogen, da sie wichtige Akteure im System des vorbeugenden personellen Sabotageschutzes im militärischen Sicherheitsbereich sind. Anders als im öffentlichen und nichtöffentlichen Bereich wurde im militärischen Sicherheitsbereich auf eine Befragung aller Sicherheitsbeauftragten verzichtet, da nicht alle Sicherheitsbeauftragten eine besonders sicherheitsempfindliche Stelle gemäß § 1 Abs. 4 S. 1 SÜG in ihrem Verantwortungsbereich betreuen. Folglich erhielten nur solche Sicherheitsbeauftragten einen Fragebogen, die auch Berührungspunkte mit dem vorbeugenden personellen Sabotageschutz im Rahmen ihrer Tätigkeit haben.

Eine weitere Neuerung gegenüber der vorherigen Evaluation stellte die **vertiefende Analyse ausgewählter Vorgänge (Fallstudien)** dar, die im Mai und Juni 2017 vom InGFA beim BfV in Köln durchgeführt wurde. Mit Hilfe dieses Instruments wurden zusätzliche Daten zu den zu evaluierenden Eingriffsmaßnahmen (besondere Auskunftsverlangen sowie IMSI-Catcher) gewonnen, die eine umfassendere Betrachtung der jeweiligen Maßnahmen ermöglichten. Anhand konkreter Vorgänge, die in Abstimmung mit BfV anhand vorher definierter Kriterien ausgewählt wurden, sollte analysiert werden, welche denkbaren Alternativen zur Ausübung der relevanten Befugnis vorab geprüft, wie die Ergebnisse des Eingriffs weiterverwendet und welche Folgemaßnahmen ergriffen wurden. Die Fallstudienanalyse stellte sich insoweit als im Ergebnis nur begrenzt taugliches Mittel dar (siehe hierzu ausführlich Kapitel 6, S. 145 f.).

Parallel zur Datenerhebung erfolgte die Vorbereitung der **rechtswissenschaftlichen Analyse**, die anschließend in der rechtlichen Bewertung der Anwendungspraxis der evaluierten Regelungen konkretisiert wurde. Gemäß dem erteilten Auftrag wurde die Verfassungskonformität der evaluierten Regelungen nicht untersucht. Zudem wurde im Zuge der Hinweise der Nachrichtendienste auf widersprüchliche Anforderungen im System der zu untersuchenden Befugnisse dieses in Rücksprache mit dem BMI einer Konsistenzbetrachtung unterworfen.

Im letzten Schritt wurden die mittels der oben beschriebenen Erhebungsinstrumente gewonnenen Daten ausgewertet, den zuvor festgelegten Prüfkriterien zugeordnet und schließlich mit den Ergebnissen der rechtswissenschaftlichen Analyse zusammengeführt. Im Folgenden werden die Ergebnisse der empirischen und rechtswissenschaftlichen Analyse jeweils für die evaluierten Regelungen vorgestellt.

4. Empirische und rechtswissenschaftliche Analyse der Anwendungspraxis der zu evaluierenden Regelungen

4.1. § 3 Abs. 1 Nr. 4 BVerfSchG, § 5 Abs. 2 BVerfSchG, § 1 Abs. 1 S. 2 MADG (mit Folgeänderung in § 18 Abs. 1 BVerfSchG)

4.1.1. Genese der Regelungen

Der sich auf „Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 GG), insbesondere gegen das friedliche Zusammenleben der Völker (Art. 26 Abs. 1 GG) gerichtet sind“ beziehende § 3 Abs. 1 Nr. 4 BVerfSchG wurde im Zuge des TBG 2002 neu eingefügt[5] und blieb seitdem unverändert. Der Gesetzgeber hielt die Aufnahme der Vorschrift für geboten, da die genannten Bestrebungen ein gefährlicher Nährboden für den wachsenden Terrorismus seien.[6] Die Vorschrift hat praktische Bedeutung. Insbesondere Auskunftsbegehren nach § 8a Abs. 2 BVerfSchG wurden schwerpunktmäßig zusammen auf § 3 Abs. 1 Nr. 3, 4, BVerfSchG, in wenigen Fällen allein auf Nummer 4 gestützt.[7]
§ 1 Abs. 1 MADG wurde durch das TBG um einen Satz 2 ergänzt.[8] Dadurch ist es dem MAD möglich, Informationen über Bestrebungen zu sammeln, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind. Der Gesetzgeber wollte damit eine Anpassung an die ebenfalls erweiterte Aufgabennorm des BfV in § 3 Abs. 1 Nr. 4 BVerfSchG erreichen. Die Übertragung der Aufgabe an den MAD sah der Gesetzgeber als besonders dringlich an. Gerade die Bundeswehr und ihr Umgang mit Waffen und Sprengstoff sei für Extremisten ein attraktiver Anziehungspunkt.[9] Die Bestimmung blieb seit 2002 unverändert.
Der Gesetzgeber stützte die Novellierung des MADG durch das TBG im Jahre 2002 auf die Kompetenzvorschriften des Bundes in Art. 73 Abs. 1 Nr. 1 und Nr. 10b GG.[10]

4.1.2. Empirische Ergebnisse

BfV

§ 3 Abs. 1 BVerfSchG legt die Aufgaben fest, welche die Verfassungsschutzbehörden des Bundes und der Länder erfüllen sollen. Bis zur Verabschiedung des TBG im Jahr 2002 waren sie für die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben,
2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,

[5] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, in Kraft getreten am 01.01.2002.
[6] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 36.
[7] Vgl. PKGr, BT-Drs. 18/216, S. 8, 9: Bericht für das Jahr 2012; PKGr, BT-Drs. 17/12774, S. 5: Bericht für das Jahr 2011; PKGr, BT-Drs. 17/8638, S. 5, 6: Bericht für das Jahr 2010; PKGr, BT-Drs. 17/4277, S. 5, 7: Bericht für das Jahr 2009.
[8] Art. 2 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 363, in Kraft getreten am 01.01.2002.
[9] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 42.
[10] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 37.

3. Bestrebungen im Geltungsbereich dieses Gesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,

zuständig. Im Rahmen der Verabschiedung des TBG im Jahr 2002 wurde die Aufgabennorm durch die Ergänzung der Nummer 4 (Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 GG), insbesondere gegen das friedliche Zusammenleben der Völker (Art. 26 Abs. 1 GG) gerichtet sind) weiter konkretisiert. Darüber hinaus wurde durch die Ergänzung des § 3 Abs. 1 BVerfSchG auch der Verweis in § 5 Abs. 2 BVerfSchG geändert.
Eine Aussage darüber, wie häufig der Verfassungsschutz sich bei seinen Aktivitäten im Evaluationszeitraum auf die jeweiligen Regelungen gestützt hat, ist an dieser Stelle nicht möglich, da hierzu keine Statistiken existieren und für den Erhebungszeitraum auch nicht verlässlich und nur mit sehr erheblichem Aufwand vom BfV hätten geführt werden können.[11] So war es lediglich möglich, im Zusammenhang mit den evaluierungspflichtigen Befugnisnormen (§ 8a-c BVerfSchG sowie § 9 Abs. 4 BVerfSchG) Erkenntnisse zur Anwendungshäufigkeit von § 3 Abs. 1 Nr. 4 BVerfSchG zu gewinnen, da dort erfasst wurde, wie oft die Befugnis sich (auch) auf diese Aufgabe bezog (siehe Kapitel 4.2., S. 20 ff. bzw. Kapitel 4.3., S. 53 ff.).

BAMAD

Analog zum BVerfSchG erfolgte auch eine Änderung der Aufgabennorm im MADG. So wurde in § 1 Abs. 1 MADG der Satz 2 mit folgendem Wortlaut angefügt:

> „Darüber hinaus obliegt dem Militärischen Abschirmdienst die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über die Beteiligung von Angehörigen des Geschäftsbereiches des Bundesministeriums der Verteidigung sowie von Personen, die in ihm tätig sind oder in ihm tätig sein sollen, an Bestrebungen, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Abs. 1 des Grundgesetzes) gerichtet sind."

Anders als beim BfV sind für das BAMAD konkretere Aussagen zur Anwendungshäufigkeit der neu eingefügten Regelung möglich. Im Erhebungszeitraum stützte sich der Nachrichtendienst der Bundeswehr bei der Durchführung nachrichtendienstlicher Operationen[12] in erster Linie (in rund 85 Prozent der Fälle) auf § 1 Abs. 1 S. 1 MADG, während § 1 Abs. 1. S. 2 MADG deutlich weniger (in rund 15 Prozent der Fälle) zur Anwendung kam. Das BAMAD wies in diesem Zusammenhang daraufhin, dass vor allem die nachrichtendienstlichen Operationen, die sich auf § 1 Abs. 1 S. 2 stützen würden, aufgrund des zumeist sensiblen Umfeldes und besonderen Gefährdungspotenzials erhebliche Ressourcen binden und deutlich umfangreichere Maßnahmen nach sich ziehen würden. Als Beispiel wurde der Fall eines Bundeswehrangehörigen

[11] Da alle Fachabteilungen sich bei ihrer Arbeit auf die Aufgabennorm stützen, wäre es erforderlich gewesen, dass alle operativ tätigen Mitarbeiterinnen und Mitarbeiter die Anwendungsfälle der Norm hätten händisch erfassen müssen. Zudem wäre es problematisch gewesen, eine passende Bezugsgröße für die Erfassung der Anwendungsfälle zu finden, da – anders als im Polizeibereich – im nachrichtendienstlichen Bereich nicht von „Fällen" gesprochen werden kann.
[12] Nachrichtendienstliche Operationen werden dann aufgenommen, wenn tatsächliche Anhaltspunkte (§ 1 Abs. 1 S. 3 MADG i. V. m. § 4 Abs.1 S. 3 BVerfSchG) für Bestrebungen oder Tätigkeiten nach § 1 Abs. 1 MADG vorliegen. Im Rahmen einer nachrichtendienstlichen Operation können sowohl offene Ermittlungen als auch nachrichtendienstliche Mittel zum Einsatz kommen.

genannt, der in seiner Freizeit für die PKK im Nordirak gegen den Islamischen Staat kämpfe. Zudem beantragte das BAMAD G 10-Maßnahmen mehrheitlich auf dieser Grundlage.
Im Erhebungszeitraum stützte sich das BAMAD allerdings bei keiner Datenerhebungsmaßnahme gemäß § 4a MADG i. V. m. § 8a-c BVerfSchG bzw. § 5 MADG i. V. m. § 9 Abs. 4 BVerfSchG auf § 1 Abs. 1 S. 2 MADG (siehe Kapitel 4.2.2.3., S. 33 ff.).

Bewertung durch BfV und BAMAD

Nach Aussage des BfV und des BAMAD wird die Neuregelung insgesamt positiv bewertet, da durch sie die bisherige Aufgabennorm ergänzt wird und somit für das Tätigwerden im Bereich des internationalen Terrorismus eine ergänzende Grundlage bietet. Das BfV verweist darauf, dass die Aufgabenkonkretisierung eine hohe Bedeutung für die nachrichtendienstliche Arbeit – vor allem im Bereich des legalistischen Islamismus und des Ausländerextremismus – habe. In der Regel stütze sich das Tätigwerden des BfV zunächst auf § 3 Abs. 1 Nr. 1 BVerfSchG. Dies könne allerdings dann zu Problemen führen, wenn sich die konkrete Vereinigung nicht gegen Deutschland bzw. die freiheitliche demokratische Grundordnung richte, oder der für § 3 Abs. 1 Nr. 3 BVerfSchG erforderliche Gewaltbezug fehle, sie aber weiterhin beobachtungswürdig sei, da sie auch völkerverständigungswidrige Bestrebungen verfolge. Dann sei die Nummer 4 die einzige Aufgabennorm, auf die sich das BfV noch stützen könne.
Allerdings ist festzustellen, dass die Neuregelung im Erhebungszeitraum immer in Verbindung mit weiteren Aufgabennormen – vor allem mit den Nummern 1 und 3 des § 3 Abs. 1 BVerfSchG – herangezogen wurde. Dies deckt sich im Wesentlichen auch mit den Ergebnissen der letzten beiden Evaluationen[13]. Aus Sicht der beiden Nachrichtendienste stellt die Neuregelung eine sinnvolle Erweiterung dar, die sich in der Praxis bewährt hat und daher beibehalten werden sollte.

4.1.3. Rechtswissenschaftliche Bewertung

Bei § 3 Abs. 1 Nr. 4 BVerfSchG und § 1 Abs. 1 S. 2 MADG handelt es sich um Aufgaben-, keine Befugnisnormen. Die Vorschriften ermächtigen nicht selbst zu Maßnahmen, die mit einem Grundrechtseingriff verbunden sind.
Aufgabe der Nachrichtendienste ist es vorrangig, Aufklärung im Vorfeld von konkreten Gefahren zu ergreifen. Die Ziele sind entsprechend weit gefasst, die Befugnisse dagegen beschränkt (vgl. § 8 Abs. 3 BVerfSchG). Nachrichtendienstliches Handeln ist gekennzeichnet durch niedrige Eingriffsschwellen, ein recht weites Aufgabenfeld, eine grundsätzlich geheime Datensammlung und eine deshalb eingeschränkte Möglichkeit individuellen Rechtsschutzes.
Hieraus kann allerdings nicht ohne Weiteres geschlossen werden, dass die Bestimmungen für die verfassungsrechtliche Bewertung der empirisch ermittelten Anwendungspraxis von vornherein irrelevant wären. Verschiedene zu evaluierende Regelungen, die zu grundrechtsrelevanten Maßnahmen ermächtigen, setzen voraus, dass Gefahren für die in § 3 Abs. 1 BVerfSchG bzw. § 1 Abs. 1 S. 2 MADG genannten Schutzgüter vorliegen (z. B. § 8a Abs. 1, Abs. 2, Abs. 2a BVerfSchG). Hierdurch gehört auch die Prüfung, ob eine Gefahr für das in § 3 Abs. 1 Nr. 4 BVerfSchG bzw. § 1 Abs. 1 S. 2 MADG bezeichnete Schutzgut vorliegt, zu den Tatbestandsvoraussetzungen der jeweiligen Eingriffsnorm. Die Einführung der zusätzlichen Aufgabennorm kann deshalb dazu führen, dass mehr grundrechtsrelevante Maßnahmen, auch gegenüber anderen Grundrechtsträgern und u. U. anderen Schutzgütern ergriffen werden.

[13] Vgl. BMI, Bericht der Bundesregierung zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (nur Entwurf), 2011, S. 22; Bundesregierung, BT-Dr. 18/5935, S. 17.

Die Ergebnisse der empirischen Erhebung machen eine verfassungsrechtliche Bewertung nur auf zurückgezogener Linie möglich, weil seitens des BfV keine Aufstellung über die Gesamtzahl der Fälle, in denen Maßnahmen auf eine Gefährdung der in § 3 Abs. 1 Nr. 4 BVerfSchG genannten Schutzgüter gestützt werden können, geführt worden ist. Die Auswertung der empirischen Erfassung der Maßnahmen nach § 8a Abs. 2 und 2a BVerfSchG, § 9 Abs. 4 BVerfSchG und § 4a MADG deutet darauf hin, dass § 3 Abs. 1 Nr. 4 BVerfSchG bzw. § 1 Abs. 1 S. 2 MADG nur in einer sehr geringen Zahl der Fälle als ausschließliche Schutzguttatbestände herangezogen werden. Für die untersuchten Maßnahmen zeigt sich für das BfV, dass in keinem Fall die neugeschaffene Aufgabennorm alleinige Grundlage war. Vielmehr war sie in rund 70 Prozent der Fälle zusätzliche Aufgabennorm. Das BAMAD hat rund 15 Prozent seiner nachrichtendienstlichen Operationen auf die neue Befugnisnorm gestützt, was zeigt, dass § 1 Abs. 1 S. 2 MADG zwar eine eigenständige, jedoch im Vergleich mit den übrigen Aufgabennormen eine – rein quantitativ betrachtet – geringere Bedeutung hat.

4.2. § 8a-c BVerfSchG, § 3 BNDG, § 4a MADG

4.2.1. Genese der Regelungen

Die Vorgängernormen von §§ 8a, 8b BVerfSchG wurden im Jahre 2002 neu als § 8 Abs. 5-12 BVerfSchG eingefügt.[14] Die Maßnahmevoraussetzungen nahmen Bezug auf § 3 Abs. 1 G 10, wonach tatsächliche Anhaltspunkte für eine bestimmte Straftat vorliegen mussten. Das TBEG 2007 löste den Bezug zum Strafrecht und verortete die Bestimmungen in § 8a Abs. 4-8 BVerfSchG.[15] § 8a Abs. 9 BVerfSchG zitierte den Art. 10 GG. Die verfahrensrechtlichen Vorgaben wurden im Zuge der Novellierung im Jahre 2011 in den § 8b BVerfSchG ausgegliedert und das Zitiergebot durch § 8c BVerfSchG erfüllt.[16] Gleichzeitig erfolgte die Streichung des Auskunftsersuchens gegenüber Postdienstleistern, da die Maßnahme praktisch nicht zur Anwendung kam.[17]

a) § 8a Abs. 1 BVerfSchG, § 3 BNDG, § 4a MADG – Bestandsdatenauskunft

Das TBG ermöglichte mit § 8 Abs. 8 BVerfSchG a. F. eine Auskunft über Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten. Eine Bestandsdatenauskunft war nicht vorgesehen.[18] Dies änderte sich durch das TBEG im Jahre 2007 und die Einführung in § 8a Abs. 1 BVerfSchG.[19] Die Ursprungsnorm ermöglichte zunächst Auskünfte gegenüber den Betreibern von Telediensten und Postdienstleistern. Die Auskunft gegenüber Postdienstleistungen wurde im Jahre 2011 gestrichen[20], weil die Befugnis zum Abruf von Bestandsdaten zu Postdienstleistungen im Jahre 2009 nicht zur Bekämpfung des Terrorismus genutzt worden war (siehe Kapitel 5.3.7, S. 143). Früher genügte es für die Bestandsdatenauskunft, wenn dies zur Sammlung und Auswertung der Informationen erforderlich war[21]. Der Gesetzgeber hat im

[14] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[15] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2, in Kraft getreten am 11.01.2007.
[16] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012.
[17] Vgl. BMI, Bericht der Bundesregierung zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (nur Entwurf), 2011, S. 48.
[18] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[19] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2, in Kraft getreten am 11.01.2007.
[20] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2576, in Kraft getreten am 10.01.2012.
[21] Bundesregierung, BT-Drs. 17/6925, S. 12.

Jahre 2011 vorgesehen, dass nunmehr zusätzlich „tatsächliche Anhaltspunkte für schwerwiegende Gefahren“ bestehen müssen, um die rechtsstaatliche Absicherung zu erhöhen.[22] An das Merkmal tatsächlicher Anhaltspunkte sind geringere Anforderungen zu stellen als an das Erfordernis bestimmter Tatsachen.[23]

b) § 8a Abs. 2 BVerfSchG – Auskunftsersuchen in weiteren Fällen

Im Jahre 2011 wurde die Befugnis zur Auskunft über Flugdaten und Finanztransferdaten ausgeweitet und durch einen neuen Abs. 2a die Auskunft über Kontostammdaten ermöglicht. Dies geht auf die Vorschläge des Rambøll-Gutachtens zurück.[24] Ferner wurden die Anforderungen in tatsächlicher Hinsicht verschärft (s. u. unter *sonstige Maßnahmevoraussetzungen*).

(1) § 8a Abs. 2 S.1 Nr.1 BVerfSchG – Flugdaten

Die Vorschrift wurde durch das TBG im Jahre 2002 als § 8 Abs. 7 BVerfSchG eingeführt. Sie ermöglichte „bei Luftfahrtunternehmen unentgeltliche Auskünfte zu Namen, Anschriften und zur Inanspruchnahme von Transportleistungen und sonstigen Umständen des Luftverkehrs“ einzuholen.[25] Das TBEG nahm die Vorschrift als § 8a Abs. 2 S. 1 Nr. 1 BVerfSchG auf und ermächtigte zu Auskünften von „Luftfahrtunternehmen zu Namen und Anschriften des Kunden sowie zur Inanspruchnahme und den Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg.“ [26] Das Änderungsgesetz 2011 sieht neben der Auskunft von Luftfahrtunternehmen auch eine Inanspruchnahme der „Betreiber von Computerreservierungssystemen und Globalen Distributionssystemen für Flüge“ vor.[27] Im Folgenden werden die betroffenen Daten als Flugdaten bezeichnet.

(2) § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG – Finanztransferdaten

Das TBG ermächtigte im Jahre 2002 zur Auskunft über Finanztransferdaten in § 8 Abs. 5 BVerfSchG a. F. [28] Die Einführung wurde für dringend erforderlich gehalten. Sie diente der Umsetzung der Resolution 1373 (2001) des UN-Sicherheitsrats zur Unterbindung der Finanzströme terroristischer Organisationen.[29] Die Vorschrift wurde im Zuge des TBEG im Jahre 2007 nach § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG verlagert, inhaltlich erweitert und die näheren Voraussetzungen des Eingriffs § 8a Abs. 2 S. 1 BVerfSchG a. E. zugeordnet.[30]
Die Vorschrift erlaubt Auskünfte bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen, insbesondere über Kontostand, Zahlungsein- und -ausgänge. Im Folgenden werden diese als Finanztransferdaten, in Abgrenzung zu den Kontostammdaten in § 8a Abs. 2a BVerfSchG, bezeichnet.

---

[22] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 12. Dies begrüßend Wolff/Mundil, ZG 2012, 278 (281).
[23] Vgl. BVerfG, NJW 2013, 1499 (1515) zu § 5 Abs. 2 ATDG; BVerfG, NVwZ 2009, 96 (101 f.) zu Art. 6c Abs. 2, 3 BayVSG.
[24] Vgl. BMI, Bericht der Bundesregierung zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (nur Entwurf), 2011, S. 6 f.
[25] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[26] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, in Kraft getreten am 11.01.2007.
[27] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2576, in Kraft getreten am 10.01.2012.
[28] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[29] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 39.
[30] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2, in Kraft getreten am 11.01.2007.

(3) § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG – Verkehrsdaten

Mit dem TBG wurde im Jahre 2002 die Auskunft über Verkehrs- und Nutzungsdaten zusammen in § 8 Abs. 8 BVerfSchG a. F. erfasst.[31] Die Einführung verfolgte insbesondere den Zweck, das Umfeld des Betroffenen zu ermitteln und Informationen zu den Kommunikationsbeziehungen innerhalb der Terrororganisation zu erlangen.[32] Die Regelung über Verkehrsdaten wurde im Jahre 2007 von den Nutzungsdaten abgetrennt und inhaltlich geändert in § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG aufgenommen.[33] Die Bestimmung blieb seitdem unverändert.
Die Vorschrift enthält keine Befugnis für den Dienstleister, Daten des Kunden zu erheben oder zu speichern.[34] Durch den Verweis auf § 96 Abs. 1 S. 1 Nr. 1 Telekommunikationsgesetz (TKG) werden auch die sog. notwendigen Standortdaten erfasst.[35] Mit den „sonstigen, zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten" (ähnlich § 96 Abs. 1 S. 1 Nr. 5 TKG) sollen die Stand-by-Daten erfasst werden, da bei einem Mobilfunknetz zum Zweck des Aufbaus einer Telekommunikation zu einem Mobiltelefon dessen Standort zumindest grob bekannt sein muss. Die Angabe zu einem aktiv geschalteten Mobiltelefon kann also unabhängig vom Verbindungsaufbau erfolgen.[36] Die Vorschrift beschränkt sich jedoch nach dem objektiven Gesetzeszweck nicht darauf, sondern dient als Auffangtatbestand dazu, die Speicherung weiterer Verkehrsdaten zu ermöglichen, die sich aus der zukünftigen technischen Entwicklung ergeben könnten.[37]

(4) § 8a Abs. 2 S. 1 Nr. 5 BVerfSchG – Nutzungsdaten

Mit dem TBG wurde im Jahre 2002 die Auskunft über Verkehrs- und Nutzungsdaten einheitlich in § 8 Abs. 8 BVerfSchG a. F. normiert.[38] Im Jahre 2007 erfolgte eine Abtrennung und inhaltliche Änderung. Die Auskunft über Nutzungsdaten erhielt ihren Regelungsstandort in § 8a Abs. 2 S. 1 Nr. 5 BVerfSchG.[39] Die Vorschrift knüpft ausweislich der Gesetzesbegründung an die in § 6 Teledienstedatenschutzgesetz (TDDSG) a. F. aufgezählten Nutzungsdaten an.[40]

(5) § 8a Abs. 2 S. 1 a. E. BVerfSchG – sonstige Maßnahmevoraussetzungen

Das TBG normierte die Maßnahmevoraussetzungen für das Auskunftsersuchen in den jeweiligen Bestimmungen des § 8 Abs. 5-8 BVerfSchG a. F. gesondert.[41] Eine alle Maßnahmen umfassende Regelung wurde durch das TBEG in § 8a Abs. 2 S. 1 a. E. geschaffen.[42] Die Auskünfte konnten eingeholt werden, „soweit dies zur Aufklärung von Bestrebungen oder Tätigkeiten erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für

---

[31] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[32] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 40.
[33] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2, in Kraft getreten am 11.01.2007.
[34] Vgl. Middel, Innere Sicherheit (2007), S. 236.
[35] Vgl. Klesczewski, in: Säcker, TKG (2013), § 96 Rn. 6 f.
[36] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 15; Droste, Handbuch (2007), S. 258. Näher zum Umfang vgl. Mallmann, in: Schenke/Graulich/Ruthig, Sicherheitsrecht (2014), § 8a BVerfSchG Rn. 13 f.
[37] Vgl. Munz, in: Taeger/Gabel, BDSG, 2013, § 96 TKG Rn. 9; Klesczewski, in: Säcker, TKG (2013), § 96 Rn. 11. Vgl. auch Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011, S. 74, der von einer Abrundungs- und Ergänzungsfunktion spricht.
[38] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[39] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2, in Kraft getreten am 11.01.2007.
[40] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 15.
[41] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[42] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2, in Kraft getreten am 11.01.2007.

die in § 3 Abs. 1 BVerfSchG genannten Schutzgüter vorliegen."[43] Durch das Änderungsgesetz im Jahre 2011 wurden die Anforderungen erhöht. Zulässig ist die Auskunft, „soweit dies zur Sammlung und Auswertung von Informationen erforderlich ist und Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 3 Abs. 1 BVerfSchG genannten Schutzgüter vorliegen." Der Begriff der „tatsächlichen Anhaltspunkte" wurde ersetzt durch „Tatsachen, die die Annahme rechtfertigen", wodurch die Voraussetzungen für die Einholung von Auskünften erhöht wurden.[44] Statt von „Aufklärung von Bestrebungen oder Tätigkeiten" spricht die aktuelle Gesetzesvorschrift von der „Sammlung und Auswertung von Informationen".
Die näheren Voraussetzungen in § 8a Abs. 2 S. 2 BVerfSchG waren nicht Bestandteil des Evaluationsauftrags.

(6) § 8a Abs. 2a BVerfSchG – Kontostammdaten

Die Vorschrift ermöglicht die Einholung einer Auskunft des BfV durch das Bundeszentralamt für Steuern (BZSt) über Daten gemäß § 93b Abs. 1 Abgabenordnung (AO) i. V. m. § 24c Kreditwesengesetz (KWG) (sog. Kontostammdaten). Bereits im Zuge der TBEG-Reform 2007 wurde erwogen, die Bestimmung einzuführen. Die Bundesregierung sah in ihrem Entwurf jedoch aufgrund der unklaren Rechtslage davon ab.[45] Nach einer klärenden Entscheidung des BVerfG[46] erfolgte die Einführung im Jahre 2011.[47]

c) Verfahrensregelungen (§ 8b BVerfSchG)

Die Verfahrensregelungen zum Auskunftsverlangen wurden im Jahre 2002 in § 8 Abs. 9-12 BVerfSchG normiert[48] und durch das TBEG nach § 8a Abs. 4-8 BVerfSchG verlagert.[49] Die verfahrensrechtlichen Vorgaben wurden von den materiellen Eingriffsvoraussetzungen im Zuge der Novellierung im Jahre 2011 abgetrennt und in den neuen § 8b BVerfSchG ausgegliedert.[50]
Die Verfahrensregelungen des § 8b BVerfSchG gelten für alle Auskunftsverlangen in § 8a Abs. 2 BVerfSchG. Für die Bestandsdatenauskunft in § 8a Abs. 1 BVerfSchG gilt die Vorschrift nur teilweise: für die Regelung über die Mitteilung und das Weitergabeverbot in Abs. 4, für das Benachteiligungsverbot in Abs. 5, die Pflicht zur Auskunftserteilung in Abs. 6, die Regelung über die Mitteilung in Abs. 7 sowie die Ermächtigung zum Erlass einer Rechtsverordnung in Abs. 8. Nicht auf die Bestandsdatenauskunft anwendbar ist die Regelung über die Anordnungszuständigkeit in Abs. 1, die Einschaltung der G 10-Kommission nach Abs. 2 und die Unterrichtung des PKGr nach Abs. 3. Im Jahr 2016 erfolgte eine begriffliche Anpassung bei der Ministerienbezeichnung.[51]

---

[43] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012.
[44] Vgl. BVerfG, NJW 2013, 1499 (1515) zu § 5 Abs. 2 ATDG; BVerfG, NVwZ 2009, 96 (101 f.) zu Art. 6c Abs. 2, 3 BayVSG.
[45] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 12.
[46] Vgl. BVerfG, NJW 2007, 2464 ff.
[47] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012.
[48] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 362, in Kraft getreten am 01.01.2002.
[49] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2 f., in Kraft getreten am 11.01.2007.
[50] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012.
[51] Art. 4, Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze vom 04.11.2016, BGBl I Nr. 52, S. 2485, in Kraft getreten am 09.11.2016.

(1) § 8b Abs. 1 BVerfSchG – Antrags- und Anordnungsbefugnis

Die Vorschrift wurde im Jahre 2007 als § 8a Abs. 4 BVerfSchG eingeführt[52] und im Jahre 2011 in den heutigen § 8b Abs. 1 BVerfSchG ausgelagert.[53] Sie bestimmt, wer für den Antrag und die Anordnung eines Auskunftsersuchens in den Fällen des § 8a Abs. 2, 2a BVerfSchG zuständig ist. § 8a Abs. 4 BVerfSchG a. F. differenzierte nach der Schwere des Grundrechtseingriffs[54]: Für die Auskunft nach § 8a Abs. 2 S. 1 Nr. 2-5 BVerfSchG musste die Anordnung vom Behördenleiter oder seinem Stellvertreter schriftlich angeordnet und begründet werden. Bei der Finanztransferdatenauskunft genügte die Anordnung durch einen Bediensteten des BfV mit der Befähigung zum Richteramt. Die Zuständigkeit für die Anordnung der Flugdatenauskunft war in einer besonderen Dienstvorschrift zu regeln, die der Zustimmung des BMI bedurfte. Im Übrigen hatte die Anordnung durch ein vom Bundeskanzler beauftragtes Bundesministerium zu erfolgen.[55] Diese vergleichsweise niedrigen Anforderungen für die Auskunft über Flugdaten wurden in der Evaluation kritisch bewertet.[56] Die Reform im Jahre 2011 hat die Differenzierung aufgehoben und die Vorschrift vereinfacht. Die Neuregelung soll dem Umstand Rechnung tragen, dass es sich bei den Maßnahmen allesamt um geheime Eingriffe handelt.[57] Anordnungen werden in den Fällen des § 8a Abs. 2, 2a BVerfSchG einheitlich vom Behördenleiter beantragt und durch das zuständige Bundesinnenministerium angeordnet. Ein Antrag des Bediensteten des BfV bzw. die Regelung in einer Dienstvorschrift sind nun nicht mehr ausreichend für eine Anordnung.

(2) § 8b Abs. 2 BVerfSchG – Mitwirkung der G-10-Kommission

Die Kontrolle durch die G 10-Kommission wurde durch das TBG in § 8 Abs. 9 BVerfSchG eingeführt.[58] Im Zuge der TBEG-Reform 2007 erfolgte die Verlagerung nach § 8a Abs. 5 BVerfSchG.[59] Die Vorschrift erhielt einen neuen Satz 6 mit einem Verwendungsverbot und einer Löschungspflicht für Daten, die bei Gefahr im Verzug erlangt wurden und welche die Kommission nachträglich als unzulässig oder für nicht notwendig erklärt hat.[60]
§ 8 Abs. 9 BVerfSchG in der Fassung von 2002 erstreckte die Kontrolle durch die G 10-Kommission auf alle heute in § 8a Abs. 2 BVerfSchG normierten Auskunftsverlangen. Das TBEG im Jahre 2007 reduzierte die Kontrolle auf Postdaten, Verkehrsdaten und Nutzungsdaten nach § 8a Abs. 2 S. 1 Nr. 3, 4, 5 BVerfSchG und damit auf Maßnahmen, die in das Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG eingreifen. Die fehlende Einschaltung der G 10-Kommission fand Kritik in der Lehre.[61] Der Gesetzgeber hat darauf reagiert und im Jahre 2011 die Kontrolle durch die G 10-Kommission auf alle Maßnahmen in § 8a Abs. 2, 2a BVerfSchG erstreckt.[62] Damit hat er die Rechtslage von 2002 wiederhergestellt.

---

[52] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2, in Kraft getreten am 11.01.2007.
[53] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012.
[54] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 15.
[55] Vgl. BGBl I Nr. 64 vom 10.1.2007, S. 2 f.
[56] Vgl. Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, April 2011, S. 84, der auf § 8a Abs. 1 Bezug nimmt, inhaltlich aber § 8a Abs. 2 S. 1 Nr. 1 BVerfSchG meint. Diese lag dem Innenausschuss als BT-Ausschussdrucksache 17 (4) 245 vor.
[57] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 14.
[58] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 362, in Kraft getreten am 01.01.2002.
[59] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 3, in Kraft getreten am 11.01.2007.
[60] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 15.
[61] Vgl. Huber, NJW 2007, 881 (882).
[62] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 15.

(3) § 8b Abs. 3 BVerfSchG – PKGr

Die Unterrichtung des PKGr wurde durch das TBG in § 8 Abs. 10 BVerfSchG eingeführt[63] und im Zuge des TBEG im Jahre 2007 wortgleich nach § 8a Abs. 6 BVerfSchG verschoben.[64] Die mit dem Änderungsgesetz 2011 getroffene Neuregelung in § 8b Abs. 3 BVerfSchG enthält geringfügige inhaltliche Änderungen:[65] Das BMI als das für die Unterrichtung zuständige Ministerium wird ausdrücklich benannt. Die Unterrichtung erfasst neben § 8a Abs. 2 BVerfSchG nunmehr auch die Auskunft über Kontostammdaten nach § 8a Abs. 2a BVerfSchG. Der Verweis auf § 10 PKGrG statt wie bisher auf § 5 PKGrG trägt der Änderung des PKGrG Rechnung.

(4) § 8b Abs. 4 BVerfSchG – Mitteilung an den Verpflichteten

§ 8b Abs. 4 S. 1 BVerfSchG regelt eine Mitteilungsbeschränkung, § 8b Abs. 4 S. 2 BVerfSchG ein Weitergabeverbot. Die Vorschrift bezieht sich auf den gesamten § 8a BVerfSchG. Der heutige § 8b Abs. 4 S. 2 BVerfSchG wurde durch das TBG als § 8 Abs. 9 S. 10 BVerfSchG eingeführt.[66] Die Vorschrift geht auf die Anregung des Innenausschusses zurück.[67] Das TBEG verlagerte die Bestimmung nach § 8a Abs. 7 BVerfSchG und ergänzte sie inhaltlich um den heutigen § 8b Abs. 4 S. 1 BVerfSchG.[68] Die Neuregelung im Jahre 2011 hat die Regelung in § 8a Abs. 7 BVerfSchG wortgleich in § 8b Abs. 4 BVerfSchG verschoben.[69]

(5) § 8b Abs. 5 BVerfSchG – Benachteiligungsverbot

Der Gesetzgeber führte § 8b Abs. 5 BVerfSchG mit dem Änderungsgesetz im Jahre 2011 ein.[70] Ausweislich der Gesetzesbegründung verfolgt die Einführung des Benachteiligungsverbots drei Zwecke:

1. Der Betroffene soll vor rechtlichen Nachteilen geschützt werden, die das Auskunftsverlangen für die Geschäftsbeziehungen zwischen ihm und den Bankdiensten haben kann.
2. Das verpflichtete Unternehmen der Finanzbranche soll von seiner Verantwortlichkeit und Haftung befreit werden, die eine Fortsetzung der Geschäftsbeziehung mit dem Betroffenen haben könnte.
3. Das nachrichtendienstliche Handeln soll geschützt werden. Der Abbruch der Geschäftsbeziehung kann dazu führen, dass die weitere Erkenntnisgewinnung gefährdet wird.[71]

Dass die Bekanntgabe nachrichtendienstlicher Untersuchungen an Dritte zu einer Benachteiligung in der Geschäftswelt führen kann, war schon in den 1990er Jahren bekannt.[72] Das

[63] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 362, in Kraft getreten am 01.01.2002.
[64] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 15.
[65] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012.
[66] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 362, in Kraft getreten am 01.01.2002.
[67] Vgl. Innenausschuss, Beschlussempfehlung, BT-Drs. 14/7830, S. 7.
[68] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 3, in Kraft getreten am 11.01.2007.
[69] Vgl. Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012; Bundesregierung, BT-Drs. 17/6925, S. 15.
[70] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012.
[71] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 15.
[72] Vgl. den Fall einer Entlassung durch den Arbeitgeber BVerwG NJW 1998, 919; Bäumler, NVwZ 1999, 855.

Rambøll-Gutachten stellte fest, dass die Auskunftserteilungen in § 8a BVerfSchG mit nachteiligen Wirkungen für den Betroffenen verbunden waren: Teilweise wurden die Betroffenen entgegen der Bitten des BfV auf eine interne Sperrliste gesetzt und konnten auf ihre Bankkonten nicht mehr zugreifen, weitere Transaktionen wurden unmöglich.[73]

(6) § 8b Abs. 6 BVerfSchG – Verpflichtung zur Auskunftserteilung

Nach § 8b Abs. 6 BVerfSchG sind die in § 8a Abs. 1 und 2 S. 1 genannten Stellen verpflichtet, die Auskunft unverzüglich, vollständig, richtig und in dem Format zu erteilen, wie sie in der Rechtsverordnung nach § 8b Abs. 8 BVerfSchG vorgeschrieben ist.
Das TBG ermöglichte es mit Einführung des § 8 Abs. 5-8 BVerfSchG a. F. Auskünfte „einzuholen". Eine ausdrückliche Verpflichtung der Diensteanbieter enthielt die Vorschrift nicht, sondern diese ergab sich erst aus der Gesetzesbegründung.[74] Mit dem TBEG wurden die Auskunftsersuchen einheitlich in § 8a Abs. 1, 2 BVerfSchG geregelt und als Befugnisnorm ausgestaltet. Die Auskunftspflicht ergab sich mittelbar aus dem Wortlaut des § 8a Abs. 7 BVerfSchG a. F. (§ 8b Abs. 4 BVerfSchG n. F.). Dies wurde im Innenausschuss 2007 sowie im Rambøll-Gutachten als unklar kritisiert.[75] Das Wolff-Gutachten empfahl, von einer Verpflichtung abzusehen, die nachträglich mit einer Ordnungswidrigkeit geahndet werden könne. Es sei zwar verfassungsrechtlich zulässig, allerdings sei die damit verbundene erhöhte Intensität der Grundrechtseingriffe zu bedenken.[76] § 8b Abs. 6 BVerfSchG wurde im Jahre 2011 eingeführt.[77] Durch die Neuregelung soll klargestellt werden, dass eine Auskunftspflicht besteht.[78] Von einer mit Bußgeld bewehrten Sanktionierung wurde abgesehen. § 8a BVerfSchG ist weiterhin als Befugnisnorm ausgestaltet.

(7) § 8b Abs. 7 BVerfSchG – Mitteilung an den Betroffenen

Die Vorläuferregelung wurde durch das TBG im Jahre 2002 als § 8 Abs. 9 S. 9 BVerfSchG eingeführt.[79] Die Einschaltung der G 10-Kommission bei der Entscheidung über die Mitteilung nach § 12 Abs. 1, 3 G 10 galt für alle Auskunftsverlangen in § 8 Abs. 5-8 BVerfSchG a. F. einheitlich. Dagegen differenzierte das TBEG bei der Frage der Mitteilungspflicht zwischen den verschiedenen Anordnungen.[80] § 8a Abs. 5 S. 8 BVerfSchG a. F. verwies für die Mitteilung über Auskunftsersuchen bezüglich Postdaten, Verkehrsdaten und Nutzungsdaten auf § 12 Abs. 1, 3 G 10. Für die Auskunft über Flugdaten und Finanztransferdaten bestand eine Mitteilungspflicht gemäß § 8a Abs. 4 S. 7 BVerfSchG a. F., sobald eine Gefährdung des Zwecks des Eingriffs ausgeschlossen werden konnte. Für die Bestandsdatenauskunft war eine Mitteilung nicht vorgesehen.

---

[73] Vgl. BMI, Bericht der Bundesregierung zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (nur Entwurf), 2011, S. 75.
[74] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 36.
[75] Vgl. Möstl, Innenausschuss, Drs. 16(4)131 A, S. 17; BMI, Bericht der Bundesregierung zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (nur Entwurf), 2011, S. 10.
[76] Vgl. Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011, S. 75. A.A. BMI, Bericht der Bundesregierung zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (nur Entwurf), 2011, S. 65.
[77] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2577, in Kraft getreten am 10.01.2012.
[78] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 16.
[79] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 362, in Kraft getreten am 01.01.2002.
[80] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 3, in Kraft getreten am 11.01.2007.

Diese Dreiteilung wurde im Zuge der TBEG-Evaluation kritisiert. Die Bundesregierung wollte in ihrem Gesetzesentwurf zum Änderungsgesetz 2011 die Differenzierung zwischen Maßnahmen in § 8a Abs. 2 S. 1 Nr. 4, 5 BVerfSchG, die in das Fernmeldegeheimnis eingreifen, und den übrigen Maßnahmen in Nr. 1, 2 und Abs. 2a zunächst fortführen. Bei den Verkehrsdaten und Nutzungsdaten sollte § 12 Abs. 1 G 10 entsprechend anwendbar sein. Für die Auskünfte über Flugdaten und Finanztransferdaten sollte eine Mitteilung unterbleiben, solange eine Gefährdung des Zwecks des Eingriffs nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist.[81] Durch das Änderungsgesetz von 2011 wurde die Bestimmung nach § 8b Abs. 7 BVerfSchG verlagert und inhaltlich verändert. Seit der Novellierung erstrecken sich die Mitteilungspflichten nach § 12 Abs. 1 G 10 auf alle Maßnahmen des § 8a BVerfSchG. Eine Einschränkung dieser Mitteilungspflichten nach Maßgabe des § 12 Abs. 1 S. 5 G 10 (Möglichkeit der endgültigen Nichtmitteilung nach Zustimmung der G 10-Kommission) ist lediglich für die Maßnahmen nach § 8a Abs. 1 und 2 S. 1 Nr. 4 und 5 BVerfSchG vorgesehen, d. h. nicht für Flug- und Finanztransferdaten (siehe Kapitel 5.3.2 und 5.3.3, S. 140 ff.).

(8) § 8b Abs. 9 BVerfSchG – Entschädigung

Für die Auskunft über Verkehrsdaten kann das verpflichtete Unternehmen eine Entschädigung nach § 8b Abs. 9 BVerfSchG verlangen. Die Regelung ist im Jahre 2011 neu in das BVerfSchG eingefügt worden.[82]
Das TBG im Jahre 2002 ermöglichte dem BfV durch § 8 Abs. 5-8 BVerfSchG die Einholung unentgeltlicher Auskunft über die Daten.[83] Eine Entschädigung war für keine der Auskunftsmaßnahmen vorgesehen. Das TBEG 2007 hat das Wort „unentgeltlich“ in § 8a Abs. 2 BVerfSchG nicht übernommen. Andererseits fand sich auch kein Hinweis auf eine entsprechende Möglichkeit der Entschädigung.[84] Im Rahmen der Strafverfolgung war und ist eine Entschädigung für die Auskunft über Verkehrsdaten nach § 23 Abs. 1 Justizvergütungs- und -entschädigungsgesetz (JVEG) i. V. m. Anlage 3 vorgesehen. Dies wurde im Jahre 2011 zum Anlass genommen, eine entsprechende Regelung in § 8b Abs. 9 BVerfSchG aufzunehmen. Dadurch soll eine Gleichbehandlung mit der strafprozessualen Regelung erreicht werden.[85]
Für die übrigen in § 8a Abs. 1, 2 BVerfSchG genannten Auskunftsmaßnahmen sieht § 8b Abs. 8 S. 2 Nr. 6 BVerfSchG vor, dass die Entschädigung durch Rechtsverordnung geregelt werden kann.

d) § 8c BVerfSchG – Einschränkungen eines Grundrechts

Das TBG erfüllte das nach Art. 19 Abs. 1 S. 2 GG erforderliche Zitiergebot durch § 8 Abs. 12 BVerfSchG.[86] Durch das TBEG erfolgte eine Verlagerung nach § 8a Abs. 9 BVerfSchG.[87] Im Zuge der Novellierung 2011 wurde die Bestimmung in die neue Norm § 8c BVerfSchG ausgegliedert.[88]

---

[81] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 2, 16.
[82] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2578, in Kraft getreten am 10.01.2012.
[83] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[84] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 2 f., in Kraft getreten am 11.01.2007.
[85] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 17.
[86] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 362, in Kraft getreten am 01.01.2002.
[87] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 3, in Kraft getreten am 11.01.2007.
[88] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2578, in Kraft getreten am 10.01.2012.

e) § 2a BNDG a. F. (nunmehr § 3 BNDG)

Ursprünglich regelte § 2a BNDG das besondere Auskunftsverlangen des BND. Er verwies auf die Bestimmungen in §§ 8a, b BVerfSchG. Anstelle der in § 3 Abs. 1 BVerfSchG genannten Schutzgüter wurde auf eine schwerwiegende Gefahr für die in § 5 Abs. 1 S. 3 Nr. 1-4 und Nr. 6 G 10 genannten Gefahrenbereiche angeknüpft. Die Vorschrift wurde mit dem TBG 2002 eingeführt.[89] Aufgrund der Änderungen des BVerfSchG im Zuge des TBEG 2007 wurde die Vorschrift entsprechend angepasst.[90] Die Vorschrift verwies seitdem auf §§ 8a, b BVerfSchG und erstreckt sich daher auch auf die Auskunft über Bestandsdaten. Das Änderungsgesetz im Jahre 2011 nahm formale Anpassungen an die geänderten § 8a, b BVerfSchG vor.[91] Ferner wurde die Norm 2016 neu gegliedert und die Eigensicherung ausdrücklich als Schutzgut aufgenommen.[92] Schließlich wurden die besonderen Auskunftsverlangen im Zuge der umfassenden Novellierung des BNDG Ende 2016 in § 3 BNDG verschoben, ohne dass eine inhaltliche Änderung vorgenommen wurde.[93]

f) § 4a MADG

§ 4a MADG wurde durch das TBEG im Jahre 2007 neu eingefügt.[94] Der Gesetzgeber bezweckte mit der Einführung eine Gleichstellung mit den Befugnissen des BfV. Dies sei erforderlich, um Sicherheitslücken im Bereich der Bundeswehr zu schließen.[95] Das Änderungsgesetz im Jahre 2011 nahm nur geringe formelle Änderungen vor.[96] Anstelle des Verweises auf § 8a BVerfSchG a. F. nimmt die Bestimmung nunmehr Bezug auf §§ 8a, b BVerfSchG. Das TBEG verwies auf die Einschränkung des Post-, Brief- und Fernmeldegeheimnisses in Art. 10 Abs. 1 GG. Da das Auskunftsersuchen über den Post- und Briefverkehr in § 8a BVerfSchG gestrichen wurde, verweist § 4a MADG nur noch auf das Grundrecht des Fernmeldegeheimnisses. Der Gesetzgeber nahm die Änderung zur Anpassung an die neu strukturierten §§ 8a-c BVerfSchG vor.[97]

4.2.2. Empirische Ergebnisse

4.2.2.1. Überblick

Im Erhebungszeitraum sind insgesamt 321 Anordnungen[98] gemäß § 8a Abs. 1, 2 und 2a BVerfSchG ergangen, von denen 313 vom BfV umgesetzt wurden. Fünf besondere Auskunftsverlangen wurden vom BAMAD und drei vom BND gestellt.
In 251 Fällen ging es um die Einholung von Auskünften zu Bestandsdaten gemäß § 8a Abs. 1 BVerfSchG. In 36 Fällen wurden Auskünfte ausschließlich bei Telekommunikationsanbietern

[89] Art. 3 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 364, in Kraft getreten am 01.01.2002.
[90] Art. 4 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 4, in Kraft getreten am 11.01.2007.
[91] Art. 3 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2579, in Kraft getreten am 10.01.2012; Bundesregierung, BT-Drs. 17/6925, S. 18.
[92] Art. 2 Nr. 1 Gesetz zum besseren Informationsaustausch bei der Bekämpfung des Internationalen Terrorismus vom 26.07.2016, BGBl I Nr. 27 vom 29.07.2016, S. 1818 mWv 30.7.2016
[93] Art. 1 Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23.12.2016, BGBl I Nr. 67 vom 30.12.2016, S. 3346.
[94] Art. 3 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 4, in Kraft getreten am 11.01.2007.
[95] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 18.
[96] Art. 2 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2578, in Kraft getreten am 10.01.2012.
[97] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 18.
[98] In einem Fall hat der BND in einer Anordnung Auskünfte zu einer bereits bekannten Kontonummer bei einem Kreditinstitut eingeholt und eine Kontostammdatenabfrage beim BZSt durchgeführt (zwei Teilanordnungen). Obwohl es sich um nur einen Antrag handelte, der jedoch aus zwei Teilanordnungen bestand, wurden beide Teilanordnungen einzeln gezählt.

eingeholt. In 15 Fällen erfolgte die Einholung von Auskünften bei Kreditinstituten und/oder Finanzdienstleistungsunternehmen sowie beim BZSt (sog. Kombi-Antrag). In einem Fall erfolgte in zwei Teilanordnungen eine Abfrage einer bereits bekannten Kontonummer bei einem Kreditinstitut und parallel eine Kontostammdatenabfrage beim BZSt. In einem weiteren Fall wurden ausschließlich Auskünfte bei einem Kreditinstitut eingeholt. In zwei Fällen handelte es sich um ein besonderes Auskunftsverlangen gegenüber Luftfahrtunternehmen.

Tab. 1: Anzahl der Anordnungen nach § 8a Abs. 1, 2 und 2a BVerfSchG

Rechtsgrundlage	Anzahl
§ 8a Abs. 1 BVerfSchG	251
§ 8a Abs. 2 S. 1 Nr. 1 BVerfSchG	1
§ 8a Abs. 2 S. 1 Nr. 2 BVerfSchG	17
§ 8a Abs. 2 S. 1 Nr. 4 BVerfSchG	36
§ 8a Abs. 2 S. 1 Nr. 5 BVerfSchG	-
§ 8a Abs. 2a BVerfSchG	16[99]
Gesamt	**321**

Die Anordnungen richteten sich in einem Drittel der Fälle an jeweils ein einzelnes Unternehmen. Ein Fünftel der Anordnungen betrafen jeweils zwei Unternehmen. In 14 Fällen wurden drei bis fünf Unternehmen um die Erteilung von Auskünften gebeten. In weiteren zehn Fällen waren es sechs bis sieben Unternehmen. Eine Anordnung im Bereich der Finanzermittlungen richtete sich an insgesamt 19 verschiedene Unternehmen.
Die folgende Tabelle gibt Aufschluss darüber, an welche Unternehmenstypen die Anordnungen im Erhebungszeitraum gerichtet waren:

Tab. 2: Art der Datenerhebungsmaßnahme nach Unternehmenstypen

Auskunftsverpflichtete Unternehmen	Anzahl Nennungen
Einholung von Auskünften über Bestandsdaten bei Telediensteanbietern	251
Einholung von Auskünften bei Luftfahrtunternehmen	1
Einholung von Auskünften bei Betreibern von Computerreservierungssystemen	-
Einholung von Auskünften bei Globalen Distributionssystemen	1
Einholung von Auskünften bei Kreditinstituten	16
Einholung von Auskünften bei Finanzunternehmen	3
Einholung von Auskünften bei Finanzdienstleistungsinstituten	13
Einholung von Auskünften bei Telekommunikationsdiensteanbietern	36

[99] Bei 15 der 16 BZSt-Abfragen handelte es sich um sog. Kombi-Anträge (13x BfV, 2x BAMAD).

Einholung von Auskünften über Verkehrsdaten bei Teledienstanbietern	-
Einholung von Auskünften beim BZSt	16
Gesamt	**337**

Im Erhebungszeitraum wurden die in § 8a BVerfSchG genannten Befugnisse hauptsächlich genutzt, um Auskünfte bei Telediensteanbietern (251) einzuholen. Deutlich weniger wurde von der Möglichkeit Gebrauch gemacht, sich zur Informationsbeschaffung an Telekommunikationsunternehmen (36), Kreditinstitute (16), an das BZSt (16), an Finanzdienstleistungsunternehmen (13), Luftfahrtunternehmen sowie Globale Distributionssysteme (je 1) zu wenden. Hingegen wurden im Erhebungszeitraum keine besonderen Auskunftsverlangen an Betreiber von Computerreservierungssystemen sowie an Telediensteanbieter bzgl. der Abfrage von Verkehrsdaten gerichtet.
Hinsichtlich des Nutzungsverhaltens lässt sich ein wesentlicher Unterschied zu den Vorjahren erkennen. Obwohl das BfV die besonderen Auskunftsverlangen – im Vergleich zu BND und BAMAD – am häufigsten nutzte, ist es zu einer Verschiebung mit Blick auf die Nutzungshäufigkeit der einzelnen Befugnisse gekommen. Während der Schwerpunkt in der Vergangenheit eindeutig auf der Einholung von Auskünften bei Telekommunikationsdiensteanbietern sowie Finanzdienstleistungsinstituten und Kreditinstituten lag, war die Besonderheit im aktuellen Erhebungszeitraum, dass die Bestandsdatenabfrage bei Telediensteanbietern gemäß § 8a Abs. 1 BVerfSchG mit großem Abstand am häufigsten genutzt wurde. Unverändert blieb dagegen die Nutzung der Möglichkeit, Daten bei Luftfahrtunternehmen abzufragen, auf die weiterhin selten zurückgegriffen wurde.

Tab. 3 gibt einen Überblick, wie oft die Befugnisse nach § 8a Abs. 2 BVerfSchG von den drei Nachrichtendiensten im Zeitraum 2002 bis 2015 genutzt wurden:

Tab. 3: Anzahl der Anordnungen der besonderen Auskunftsverlangen gemäß § 8a Abs. 2 BVerfSchG nach Nachrichtendiensten 2002-2015

Jahr	Luftfahrt-unternehmen			Finanzdienst-leister			Telekommunika-tions- und Tele-diensteanbieter			Gesamt			Jahre gesamt
	BfV	*BND*	*BAMAD*	*BfV*	*BND*	*BAMAD*	*BfV*	*BND*	*BAMAD*	*BfV*	*BND*	*BAMAD*	
2002	1			8	1		21	2	3	30	3	3	36
2003	2			14	2		9	3	2	25	5	2	32
2004	0			7	0		22	1	1	29	1	1	31
2005	0			12	0		20	0	1	32	0	1	33
2006	0			7	0		14	0	0	21	0	0	21
2007	0	0	0	5	0	0	34	2	2	39	2	2	43
2008	2	0	0	10	0	0	48	2	2	60	2	2	64
2009	1	3	0	17	1	0	54	0	1	72	4	1	77
2010	10	0	0	16	0	0	42	0	1	68	0	1	69
2011	4	0	0	17	0	0	34	0	0	55	0	0	55
2012	10	0	0	25	1	0	34	0	0	69	1	0	70
2013	7	0	1	23	1	1	54	0	0	84	1	2	87
2014	3	0	0	30	0	0	37	0	2	70	0	2	72
2015	2	0	0	18	0	2	38	0	0	58	0	2	60
Ges.	**42**	**3**	**1**	**209**	**6**	**3**	**461**	**10**	**15**	**712**	**19**	**19**	**750**
Ges.	**46**			**218**			**486**			**750**			

Änderung der allgemeinen Maßnahmevoraussetzungen

In § 8a Abs. 1 BVerfSchG wurde die Eingriffsschwelle durch den Zusatz „(…) und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 3 Abs. 1 BVerfSchG Schutzgüter vorliegen“ erhöht. In § 8 Abs. 2 BVerfSchG erfolgte durch die Änderung von „tatsächliche Anhaltspunkte“ zu „Tatsachen die Annahme rechtfertigen, dass…“ ebenfalls eine Verschärfung der Tatbestandsvoraussetzungen. Das BfV wies daraufhin, dass sich die Anforderungen für die Durchführung einer Maßnahme gemäß § 8a Abs. 1 BVerfSchG als sehr hoch darstellen und fast so hoch seien wie bei G 10-Maßnahmen. Dies gilt erst recht für Maßnahmen nach § 8a Abs. 2 BVerfSchG. Ebenso wurde die Hürde für die Nebenbetroffenen nach § 8a Abs. 3 Nr. 2 BVerfSchG derart erhöht, dass nun auf Grund bestimmter Tatsachen anzunehmen sein muss, dass sie Leistungen für eine Person nach Nr. 1 in Anspruch nehmen. Das BAMAD gab an, dass es zu einer formalen Erhöhung der Tatbestandsvoraussetzungen gekommen sei, die jedoch in der Praxis oft nicht relevant sei, da die besonderen Auskunftsverlagen oft Teil eines Maßnahmenbündels seien, das auch G 10-Maßnahmen enthalten würde. Dadurch sei die

Prüfschwelle bereits sehr hoch. Sofern jedoch eine solche Maßnahme losgelöst von G 10-Maßnahmen zum Einsatz komme, könne die Unterscheidung relevant werden.
Im Folgenden erfolgt eine differenzierte Betrachtung der einzelnen Regelungen.

4.2.2.2. § 8a Abs. 1 BVerfSchG, § 3 BNDG und § 4a MADG (Bestandsdatenauskunft bei Telediensteanbietern)

Von der Möglichkeit, bei Telediensteanbietern Auskünfte über Bestandsdaten einzuholen, machte das BfV im Erhebungszeitraum insgesamt in 251 Fällen Gebrauch, während dieses Instrument beim BND und BAMAD nicht zum Einsatz kam. Das BAMAD gab jedoch an, dass die Möglichkeit außerhalb des Erhebungszeitraums in jüngerer Vergangenheit genutzt worden sei. Hierbei habe es sich um einen Fall gehandelt, in dem Ebay um die Herausgabe der Daten eines Nutzerkontos ersucht worden sei, da über dieses Konto eingestufte Papiere angeboten worden seien. Insgesamt sei von der Möglichkeit bislang aber selten Gebrauch gemacht worden. Nach Einschätzung des BAMAD werde die Nutzung dieses Instrument in Zukunft jedoch zunehmen. Der BND verwies darauf, dass der seltene Gebrauch der Befugnis, auf den besonderen Auslandsbezug, durch den die Arbeit des BND gekennzeichnet sei, sowie auf die strenge interne Erforderlichkeitsprüfung zurückzuführen sei.
Aufgrund des deutlichen Anstiegs der Fallzahlen (2016/17: 251 gegenüber 2013/14: 12) in diesem Bereich wurde in Absprache mit dem BMI und BfV auf eine einzelfallbezogene Erfassung der Maßnahmen verzichtet. Stattdessen wurden zentrale Informationen zu den besonderen Auskunftsverlangen gemäß § 8a Abs. 1 BVerfSchG vom BfV aggregiert übermittelt. Dadurch war es nicht mehr möglich, für alle Aspekte, die im für die Einzelfallerfassung vorgesehenen Erhebungsbogen abgefragt werden sollten, abzudecken bzw. hierzu exakte Angaben zu machen.
Anders als bei den besonderen Auskunftsverlangen nach § 8a Abs. 2 und 2a BVerfSchG findet hier kein formalisiertes Verfahren Anwendung. Die Überprüfung der Voraussetzungen erfolgt durch den Sachbearbeiter. Antragsbefugt sind nur bestimmte Personen. Die Beantragung erfolgt durch die Fachabteilung bei der Abteilung 3.
Hauptsächlich wurde die Möglichkeit vom BfV dazu genutzt, Informationen im Zusammenhang mit islamistischen Aktivitäten zu erheben. Die Anordnungen richteten sich insgesamt gegen 251 Personen, wobei hier nicht näher angegeben wurde, ob es sich ausschließlich um Haupt- oder auch um Nebenbetroffene gehandelt hat. Im Rahmen der Abfragen wurden lediglich Namens- und Anschriftenfragmente erhoben.
Der Nutzen der im Rahmen der besonderen Auskunftsverlangen gewonnenen Informationen für die nachrichtendienstliche Arbeit wurde – trotz lückenhafter Rückmeldungen der jeweiligen Unternehmen – als hoch eingestuft, da Informationen zu weiteren Erreichbarkeiten der Betroffenen gewonnen werden konnten, die Weiterermittlungen ermöglichten. Die Anfragen richteten sich hauptsächlich an Facebook (239) und in deutlich weniger Fällen an Twitter und YouTube (2). In diesem Zusammenhang wies das BfV darauf hin, dass es sich bei solchen Auskunftsersuchen auf Unternehmen beschränke, mit denen eine vertrauensvolle Zusammenarbeit bestehe und die Informationen nicht an Dritte weitergeben würden. Nach Angabe des BfV dauerte es in der Regel zwei bis drei Wochen, bis die zur Auskunft verpflichteten Unternehmen die gewünschten Auskünfte erteilt haben, und wurde insgesamt als zufriedenstellend bewertet. Insgesamt habe sich die Zusammenarbeit mit den verpflichteten Unternehmen verbessert und funktioniere mittlerweile gut. Auch wenn die Zusammenarbeit gut funktionieren würde, bleibe der Prozess – verglichen mit den automatisierten Abfragen nach §§ 112 und 113 TKG – „Handarbeit“. Teilweise würden die zur Auskunft verpflichteten

Unternehmen – etwa unter Berufung auf § 3 Abs. 1 NDÜV – unterschiedliche Datenformate und Kommunikationsformen (Brief, E-Mail (teils mit Link und Passwort), PDF, ZIP etc.) nutzen. Bisher sei es nicht vorgekommen, dass ein Unternehmen die Zusammenarbeit verweigert habe. Zudem gebe es keine Hinweise auf negative Folgen für die Betroffenen.
Die Abfragemöglichkeit wurde beispielsweise dafür genutzt, um den Nutzer eines sozialen Netzwerks zu identifizieren, der auf seiner Profil-Seite eine IS-Fahne gepostet hatte. In einem anderen Fall ging es um die Gewinnung weiterer Erkenntnisse über eine geschlossene rechtsextreme Facebook-Gruppe, in der Aktivitäten in Zusammenhang mit einem Umsturz (z. B. geplante Schießübungen im Ausland) diskutiert wurden. Durch die von Facebook übermittelte IP-Adresse, die in dasselbe Land geführt habe, in der auch die Schießübungen stattfinden sollten, konnten die gewonnenen Informationen zu einer Verifizierung des o. g. Szenarios beitragen.
Mit Blick auf die Lösch- und Benachrichtigungspflichten, die im neu eingefügten § 8b BVerfSchG zusammengefasst wurden, ist festzustellen, dass es im Erhebungszeitraum in keinem Fall zu einer Löschung von Daten und auch nicht zu einer Mitteilung an Betroffene gekommen ist. Dies lag daran, dass die Erhebungsbögen zu den Maßnahmen direkt nach ihrem Abschluss ausgefüllt und ans InGFA übermittelt wurden. Zu diesem Zeitpunkt lag jedoch noch keine Entscheidung über die Mitteilung an Betroffene und die Löschung der personenbezogenen Daten vor.

4.2.2.3. § 8a Abs. 2 und 2a BVerfSchG, § 3 BNDG und § 4a MADG

Im Erhebungszeitraum wurden 55 Maßnahmen gemäß § 8a Abs. 2 und 2a BVerfSchG angeordnet, wobei 49 Anordnungen durch das BfV und je drei durch das BAMAD und den BND erfolgten.

Tab. 4: Anordnungen gemäß § 8a Abs. 2 und Abs. 2a BVerfSchG nach Nachrichtendiensten

Rechtsgrundlage	BfV	BAMAD	BND	Gesamt
§ 8a Abs. 2 S. 1 Nr. 1 BVerfSchG	-	1	-	1
§ 8a Abs. 2 S. 1 Nr. 2 BVerfSchG	13	2	2	17
§ 8a Abs. 2 S. 1 Nr. 4 BVerfSchG	36	-	-	36
§ 8a Abs. 2 S. 1 Nr. 5 BVerfSchG	-	-	-	-
§ 8a Abs. 2a BVerfSchG	13	2	1	16
Gesamt	**49**	**3**[100]	**3**	**55**[101]

[100] Bei zwei Fällen handelte es sich um Kombi-Anträge (§ 8a Abs. 2a plus § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG), die hier nur einmal gezählt werden.
[101] Bei 15 der 16 BZSt-Abfragen handelte es sich um Kombi-Anträge, die hier nur einmal gezählt werden.

Gründe für die Datenerhebung

Für den Einsatz der Datenerhebungsmaßnahmen wurden dabei folgende Gründe genannt:

Tab. 5: Gründe für die Datenerhebung gemäß § 8a Abs. 2 und 2a BVerfSchG[102]

Gründe für die Anordnung der Maßnahme	**Anzahl der Nennungen** (Mehrfachnennungen möglich)
Aufgrund von Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben (§ 3 Abs. 1 Nr. 1 BVerfSchG)	29[103]
Aufgrund von Bestrebungen, die bezwecken oder auf Grund ihrer Wirkungsweise geeignet sind, zu Hass oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumden anzugreifen und dadurch die Bereitschaft zur Anwendung von Gewalt zu fördern und den öffentlichen Frieden zu stören oder (§ 3 Abs. 1 Nr. 1 i. V. m. § 8a Abs. 2 S. 2 Nr. 1 BVerfSchG)	*(-)*
Aufgrund von Bestrebungen, die bezwecken oder auf Grund ihrer Wirkungsweise geeignet sind, Gewalt anzuwenden oder vorzubereiten, einschließlich dem Befürworten, Hervorrufen oder Unterstützen von Gewaltanwendung, auch durch Unterstützen von Vereinigungen, die Anschläge gegen Personen oder Sachen veranlassen, befürworten oder androhen (§ 3 Abs. 1 Nr. 1 i. V. m. § 8a Abs. 2 S. 2 Nr. 2 BVerfSchG)	(27)
Aufgrund von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht (§ 3 Abs. 1 Nr. 2 BVerfSchG)	10
Aufgrund von Bestrebungen im Geltungsbereich dieses Gesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden (§ 3 Abs. 1 Nr. 3 BVerfSchG)	36

[102] Die 15 Kombi-Anträge von BfV und BAMAD wurden hier nur jeweils einmal gezählt.
[103] In zwei Fällen wurden keine weiteren Angaben gemacht, um welche Bestrebungen es sich genau handelte.

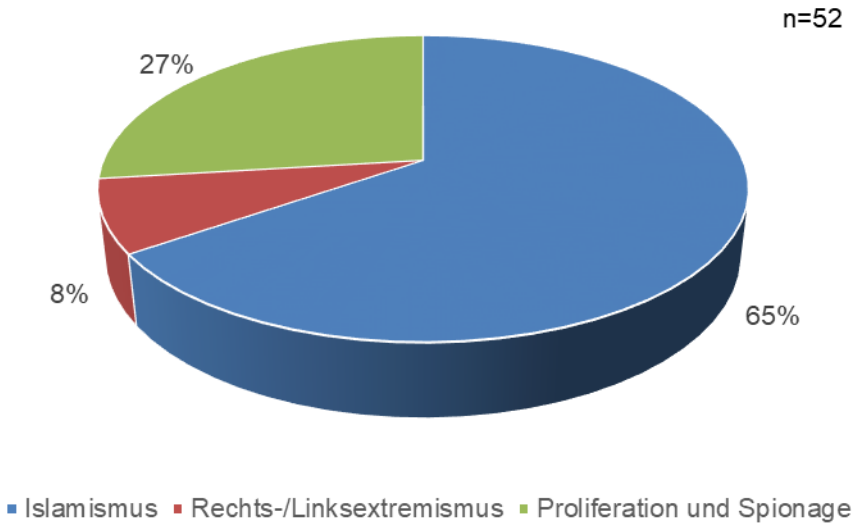
Aufgrund von Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Abs. 1 des Grundgesetzes) gerichtet sind. (§ 3 Abs. 1 Nr. 4 BVerfSchG)	34
Zum Schutz von Mitarbeitern, Einrichtungen, Gegenständen und Quellen des BND gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten (§ 3 Abs. 1 S. 1 Nr. 2 BNDG)	3
Aufgrund von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht (§ 1 Abs.1 S. 1 Nr. 2 MADG)	3
Gesamtzahl	**115**

Die wichtigsten Aufgabennormen, auf die das BfV seine Anträge gemäß § 8a Abs. 2, 2a BVerfSchG im Erhebungszeitraum stützte, waren § 3 Abs. 1 Nr. 3 BVerfSchG (36), § 3 Abs. 1 Nr. 4 BVerfSchG (34) sowie § 3 Abs. 1 Nr. 1 BVerfSchG (29). Seltener wurde hingegen auf § 3 Abs. 1 Nr. 2 BVerfSchG zurückgegriffen. Das BAMAD stützte sich bei seinen Anträgen ausschließlich auf § 1 Abs.1 S. 1 Nr. 2 MADG, während der BND im Erhebungszeitraum immer auf § 3 Abs. 1 Nr. 2 BNDG zurückgriff.
Bei 21 Anträgen stützten sich die drei Nachrichtendienste auf eine einzige Aufgabennorm. In elf Fällen griff das BfV auf zwei Aufgabennormen zurück, um Anträge gemäß § 8a Abs. 2 und 2a BVerfSchG zu stellen. Drei Aufgabennormen dienten in 21 Fällen als Begründung für die Anträge des BfV. Zweimal wurde auf alle vorhandenen Aufgabennormen im Bundesverfassungsschutzgesetz zurückgegriffen.
Der evaluierungspflichtige § 3 Abs. 1 Nr. 4 BVerfSchG diente regelmäßig als zusätzliche Begründung, jedoch stützte sich das BfV in keinem Fall ausschließlich auf diese Aufgabennorm. Am häufigsten wurde § 3 Abs. 1 Nr. 4 BVerfSchG in Verbindung mit den Nummern 1 und 3 (21) als Grundlage für Anträge gemäß § 8a Abs. 2 und 2a BVerfSchG genutzt. In zehn Fällen war es zusätzlich nur die Nummer 3. In einem Fall begründete die Nummer 4 mit der Nummer 1 zusammen den Antrag für die Durchführung einer Maßnahme gemäß § 8a Abs. 2 und 2a BVerfSchG. Eine Begründung, die sich auf alle Aufgabennormen des BfV stützte, gab es im Erhebungszeitraum nur zweimal.
Das BAMAD nannte in keinem Fall den analog zu § 3 Abs. 1 Nr. 4 BVerfSchG eingeführten § 1 Abs. 1 S. 2 MADG als Grund für die im Erhebungszeitraum durchgeführten Datenerhebungsmaßnahmen.

Zuordnung zu Phänomenbereichen

Hinsichtlich der Zuordnung der angeordneten Maßnahmen zu einzelnen Phänomenbereichen zeigte sich ein eindeutiger Schwerpunkt: Der Großteil der Anordnungen sind dem Phänomenbereich Islamismus (34) zuzuordnen, während die Bereiche Proliferation und Spionage (14) und Rechts- und Linksextremismus (4) im Erhebungszeitraum nur eine untergeordnete Rolle spielten.

Abb. 1: Anordnungen nach Phänomenbereichen[104]



Hinsichtlich der Gefahrenlagen im Bereich des *Islamismus* ging es dabei überwiegend um die Unterstützung von islamistischen/terroristischen Organisationen und Vereinigungen bzw. um die Unterstützung von terroristischen Aktivitäten. Im Bereich *Proliferation und Spionage* waren es vor allem der Verdacht geheimdienstlicher Tätigkeiten im Geltungsbereich des BVerfSchG (BfV) bzw. die Aufdeckung ungewöhnlicher Zahlungen, die als Entgelt für eine Spionagetätigkeit anzusehen sind, sowie die Klärung von Agentenlohn (BAMAD). Im Phänomenbereich *Rechts-/Linksextremismus* ging es um die Unterstützung eines gewaltorientierten linksextremistischen Personenzusammenschlusses, die Planung, Vorbereitung und Durchführung von gegen linksorientierte Einrichtungen und Personen gerichtete Straftaten, Unterstützung einer ausländischen terroristischen Organisation sowie die Planung, Vorbereitung und Durchführung von gegen islamische Einrichtungen und Personen gerichtete Gewalttaten.

Betroffene

Im Erhebungszeitraum richteten sich die durch das BMI, das Bundeskanzleramt (BKAmt) und das BMVg angeordneten besonderen Auskunftsverlangen gegen insgesamt **110 Personen** (BfV: 103 Personen; BND: 3 Personen und BAMAD: 4 Person). Beim Großteil der Personen handelte es sich um Hauptbetroffene (81), bei denen tatsächliche Anhaltspunkte dafür vorlagen, dass sie die schwerwiegenden Gefahren nach § 8a Abs. 2 oder 2a BVerfSchG bzw. die in § 5 Abs. 1 S. 3 Nr. 1 bis 4 und 6 G 10 genannten Gefahrenbereiche nachdrücklich fördern (§ 8a Abs. 3 Nr. 1 BVerfSchG) (BfV: 75 Personen; BND: 3 Personen und BAMAD: 3 Personen). Bei den übrigen 29 Personen handelte es sich um Nebenbetroffene. Bei 20 Personen (alle BfV) hiervon bestand der Verdacht, dass sie Nachrichten für Hauptbetroffene entgegennehmen oder weitergeben oder diese ihren Anschluss nutzen würden (§ 8 Abs. 3 Nr. 2b BVerfSchG). Bei neun Personen (BfV: 8 und BAMAD: 1) bestand der Verdacht, dass sie Leistungen für einen Hauptbetroffenen in Anspruch nehmen würden (§ 8 Abs. 3 Nr. 2a BVerfSchG).

[104] Für den BND erfolgte keine Abfrage des Phänomenbereichs. Daher wurden diese Fälle hier nicht berücksichtigt.

Tab. 6: Anzahl und Art der Personen, gegen die sich die Anordnung gemäß § 8a Abs. 2 und 2a BVerfSchG richtete

Anzahl der Personen	Gesamt
Person(en), bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie die schwerwiegenden Gefahren nach den Absätzen 2 oder 2a nachdrücklich fördern	81
Person(en), bei denen auf Grund bestimmter Tatsachen anzunehmen ist, bei Auskünften nach Absatz 2 Satz 1 Nr. 1, 2 und 5 sowie nach Absatz 2a, dass sie die Leistung für eine Person nach Nummer 1 in Anspruch nehmen	9
Person(en), bei denen auf Grund bestimmter Tatsachen anzunehmen ist, bei Auskünften nach Absatz 2 Satz 1 Nummer 4, dass sie für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben, oder dass eine Person nach Nummer 1 ihren Anschluss benutzt	20
Gesamt	**110**

Im Durchschnitt richtete sich damit jede Anordnung gegen zwei Personen.
Beim Großteil der Anordnungen (48) wurde vom Behördenleiter bzw. seinem Stellvertreter kein Verlängerungsantrag gestellt. In sieben Fällen wurde ein solcher Antrag gestellt und auch genehmigt. Vier Anordnungen wurden dabei für drei Monate verlängert, während eine Anordnung drei Mal für jeweils drei Monate verlängert wurde. In zwei Fällen erfolgte keine Angabe zum Verlängerungszeitraum.

Von den Nachrichtendiensten erhobene Daten

Hinsichtlich der im Rahmen der besonderen Auskunftsverlangen gewonnenen Daten wird deutlich, dass mit Blick auf den Datenumfang vor allem die Verkehrsdatenabfrage bei Telekommunikationsanbietern im Erhebungszeitraum eine große Rolle spielten, da hierbei insgesamt die meisten Informationen erhoben wurden. Umfangreiche Informationen wurden auch im Rahmen von Finanzermittlungen mittels Kombi-Anträgen, die sowohl an das BZSt und an Kreditinstitute, Finanzdienstleistungsunternehmen und Finanzunternehmen gerichtet waren, erhoben.
In der folgenden Tabelle wird dargestellt, wie oft welche Einzeldaten bei welchem Unternehmenstyp abgefragt wurden. So kann etwa die Abfrage bei einem TK-Diensteanbieter von einem Datum (z. B. Nummer) bis hin zu einem ganzen Strauß an Daten (zusätzlich Kartennummer, Standortdaten etc.) reichen. Wie viele Daten bei welcher konkreten Abfrage erhoben wurden, kann nicht abgelesen werden, doch lassen sich durchaus typische Abfragemuster erkennen. Zudem wurde eine Unterteilung nach Typen von Betroffenen vorgenommen (a, b, c).

Tab. 7: Informationen, die gemäß § 8a Abs. 2 und 2a BVerfSchG erhoben wurden

a = Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie die schwerwiegenden Gefahren nach den Absätzen 2 oder 2a nachdrücklich fördern
b = Personen, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, bei Auskünften nach Absatz 2 Satz 1 Nr. 1, 2 und 5 sowie nach Absatz 2a, dass sie die Leistung für eine Person nach Nummer 1 in Anspruch nehmen
c = Personen, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, bei Auskünften nach Absatz 2 Satz 1 Nummer 4, dass sie für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Mitteilungen entgegennehmen oder weitergeben, oder dass eine Person nach Nummer 1 ihren Anschluss benutzt

Erhobene Daten/Personen	**a**	**b**	**c**	**Gesamt**
Telekommunikationsdiensteanbieter (36 Abfragen[105])	**324[106]**	**-**	**143**	**467**
Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung	36	-	16	52
personenbezogene Berechtigungs-kennungen	-	-	-	-
Kartenummer (bei der Verwendung von Kundenkarten)	4	-	-	4
Standortdaten (bei mobilen Anschlüs-sen)	36	-	16	52
Verbindungsdaten nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Daten-mengen	36	-	16	52
Vom Nutzer in Anspruch genommener Telekommunikationsdienst	36	-	16	52
Endpunkte von festgeschalteten Verbin-dungen	36	-	16	52
Beginn und Ende der festgeschalteten Verbindungen nach Datum und Uhrzeit	35	-	16	51
Übermittelte Datenmengen, soweit davon Entgelte abhängigen	35	-	15	50
Sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunika-tion sowie zur Entgeltabrechnung notwendige Verkehrsdaten	35	-	16	51

[105] Die Zahl der Abfragen ergibt sich aus Tabelle 2.
[106] In dieser Zeile findet sich die Summe der Einzeldaten. Dies gilt für alle grau hinterlegten Zeilen.

Sonstige Daten, davon:	35	-	16	51
IMEI, IMSI bei Mobilfunkgeräten	*35*	-	*16*	*51*
Luftfahrtunternehmen (1 Abfrage)	**1**	**-**	**-**	**1**
Name des Kunden	-	-	-	
Anschrift des Kunden	-	-	-	
Zeitpunkt der Abfertigung	-	-	-	
Zeitpunkt des Abfluges	-	-	-	
Buchungsweg	-	-	-	
Sonstige Daten, davon:	1	-	-	1
Flug-Nr.	*1*	-	-	*1*
Buchungscode	*1*	-	-	*1*
Ticket-Nr.	*1*	-	-	*1*
Datum und Zeit der Flüge	*1*	-	-	*1*
Start- und Zielflughafen	*1*	-	-	*1*
Hinweis auf die Durchführung durch eine andere Fluggesellschaft	*1*	-	-	*1*
Buchungsdatum	*1*	-	-	*1*
Telefonnummer	*1*	-	-	*1*
E-Mail-Adresse	*1*	-	-	*1*
Reiseveranstalter	*1*	-	-	*1*
Bundeszentralamt für Steuern (16 Abfragen)	**97**	**42**	**-**	**139**
Nummer eines Kontos, das der Verpflichtung zur Legitimationsprüfung im Sinne des § 154 Abs. 2 Satz 1 der Abgabenordnung unterliegt, oder Depots	15	7	-	22
Tag der Einrichtung	15	7	-	22
Tag der Auflösung	15	7	-	22
Name des Inhabers	15	6	-	21
Tag der Geburt des Inhabers (bei natürlichen Personen)	15	6	-	21
Name eines Verfügungsberechtigten	15	6	-	21

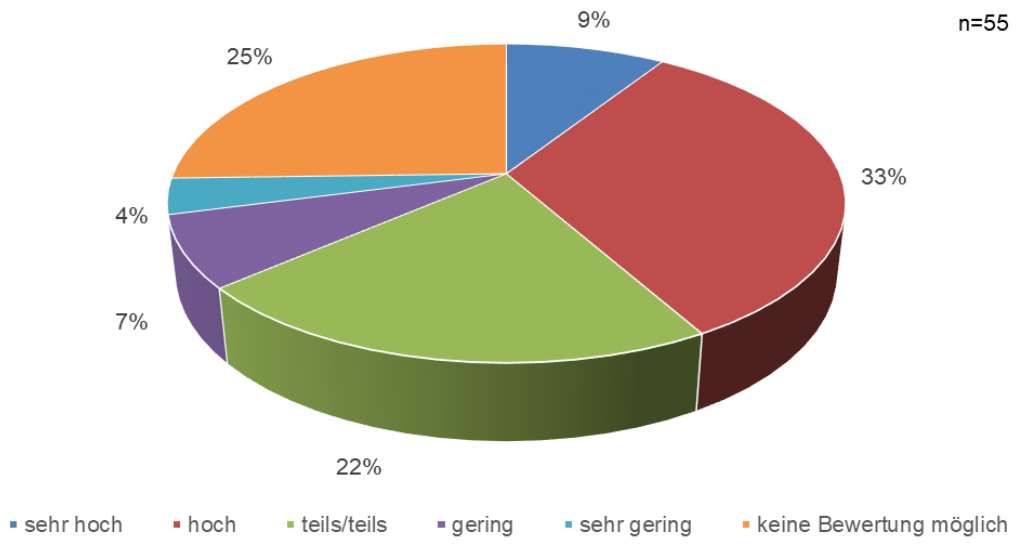
Name eines abweichend wirtschaftlich Berechtigten im Sinne des § 1 Abs. 6 des Geldwäschegesetzes	-	1	-	1
Anschrift eines abweichend wirtschaftlich Berechtigten im Sinne des § 1 Abs. 6 des Geldwäschegesetzes	-	-	-	-
Sonstige Daten, davon:	7	2	-	9
Namen der kontoführenden (Kredit-) Institute	*7*	*2*	-	*9*
Kreditinstituten (16 Abfragen)	**75**	**38**	**0**	**113**
Kontonummer	15	7	-	22
Kontoinhaber	15	6	-	21
Sonstige Berechtigte	6	3	-	9
Weitere am Zahlungsverkehr Beteiligte	5	5	-	10
Kontostand	14	7	-	21
Zahlungsein- und -ausgänge	14	7	-	21
Sonstige Daten, davon:	6	3	-	9
Kontoeröffnungsunterlagen	*4*	*3*	-	*7*
Kontoführungsunterlagen	*2*	*0*	-	*2*
Finanzunternehmen (3 Abfragen)	**12**	**3**	**-**	**15**
Kontonummer	3	1	-	4
Kontoinhaber	3	-	-	3
Sonstige Berechtigte	-	-	-	-
Weitere am Zahlungsverkehr Beteiligte	-	-	-	-
Kontostand	3	1	-	4
Zahlungsein- und -ausgänge	3	1	-	4
Sonstige Daten	-	-	-	-
Finanzdienstleistungsunternehmen (13 Abfragen)	**34**	**15**	**-**	**49**
Kontonummer	-	-	-	-
Kontoinhaber	-	-	-	-
Sonstige Berechtigte	-	-	-	-
Weitere am Zahlungsverkehr Beteiligte	13	6	-	19
Kontostand	-	-	-	-

Zahlungsein- und -ausgänge	13	6	-	19
Sonstige Daten, davon:	8	3	-	11
Persönliche Daten	*8*	*3*	-	*11*
Legitimationsdaten	*8*	*3*	-	*11*
Ort- und Zeit der Ein-/auszahlung	*8*	*3*	-	*11*
Filiale	*8*	*3*	-	*11*

Nutzen der gewonnenen Informationen für die nachrichtendienstliche Arbeit

Die Nachrichtendienste wurden im Rahmen der Erhebung zudem gebeten, für jede Anordnung den konkreten Nutzen der gewonnenen Informationen für die nachrichtendienstliche Arbeit zu bewerten. In rund 42 Prozent der Fälle wurde der Nutzen der Informationen als hoch bzw. sehr hoch eingestuft, wohingegen in knapp 11 Prozent der Fälle der Nutzen als gering bzw. sehr gering bewertet wurde. In knapp 22 Prozent waren die gewonnenen Informationen teilweise nützlich für die nachrichtendienstliche Arbeit. Bei rund einem Viertel der Anordnungen war eine Bewertung seitens des BfV nicht möglich. Eine Einschätzung des Nutzens einer Finanzermittlungsmaßnahme war nach Aussage des BfV im Evaluierungszeitraum zumeist nicht möglich, da die Verpflichteten i. d. R. die Unterlagen erst nach Abschluss des Evaluationszeitraum vollständig übersendet haben. Diese mussten zum Teil händisch erfasst und in einem ersten Schritt im Finanzermittlungsreferat ausgewertet werden. Anschließend erfolgte eine Auswertung der im Finanzermittlungsbericht enthaltenen Sachverhalte in der Fachabteilung. In der nachrichtendienstlichen Auswertung wird die gewonnene Erkenntnis eingeordnet, sodass sich erst dort der Nutzen zeigt. Das für die Finanzermittlung zuständige Referat kann den Nutzen der Maßnahme dagegen nicht abschließend einschätzen. Ein Feed-Back von den Fachabteilungen an das für Finanzermittlungen zuständige Referat war wegen der zeitlichen Streckung im Evaluationszeitraum nicht möglich.

Abb. 2: Bewertung des konkreten Nutzens der gewonnenen Informationen für die nachrichtendienstliche Arbeit

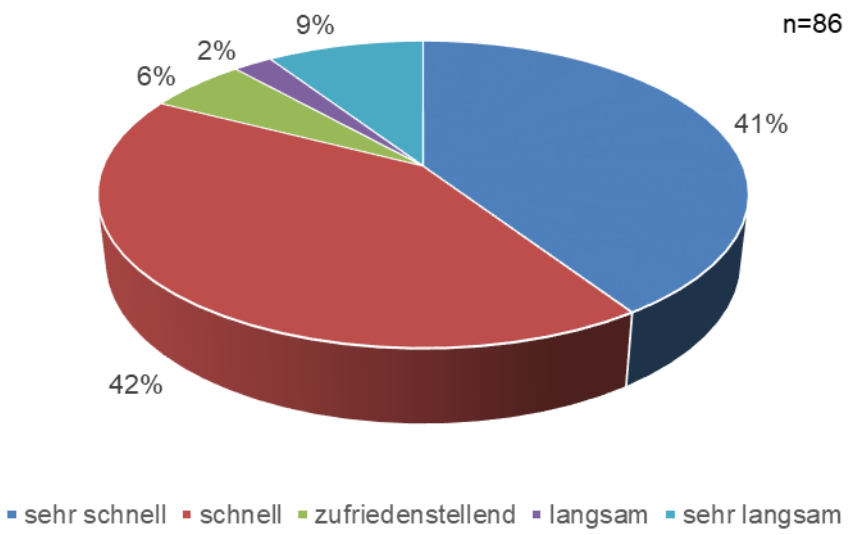


Im Anhang sind zudem einige Fallbeispiele aufgeführt, die darlegen, welcher konkrete Nutzen mit dem Einsatz der Maßnahmen nach § 8a Abs. 2 und 2a BVerfSchG verbunden war (siehe Anhang, S. 156 ff.).

Reaktionszeit der zur Auskunft verpflichteten Unternehmen

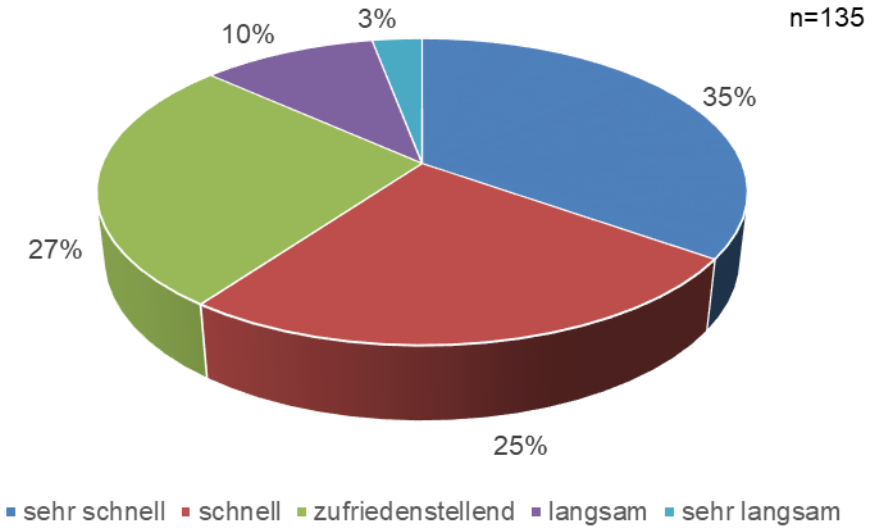
Hinsichtlich der Erfassung der Reaktionszeit, d. h. der Zeit, die die zur Auskunft verpflichteten Unternehmen benötigten, um die angeforderten Informationen zur Verfügung zu stellen, hat es gegenüber der letzten Evaluation eine methodische Anpassung im Bereich der Finanzermittlungen gegeben. Da es in diesem Bereich üblich ist, dass die zur Auskunft verpflichteten Unternehmen die angeforderten Daten in mehreren Paketen an das BfV übersenden, wurden hier – anders z. B. als bei den Telekommunikationsdiensteanbietern – nicht die einzelnen Unternehmen, sondern die Übermittlungsvorgänge pro Unternehmen erfasst. Aus diesem Grund erfolgte eine getrennte Auswertung nach § 8a Abs. 2 S.1 Nr. 2 und Abs. 2a BVerfSchG sowie nach § 8a Abs. 2 S. 1 Nr. 1 und 4 BVerfSchG zur Auskunft verpflichteten Unternehmen. Die Reaktionszeit betrug bei den nach § 8a Abs. 2 S. 1 Nr. 1 und 4 BVerfSchG zur Auskunft verpflichteten Unternehmen im Durchschnitt neun Tage, wobei die Spannbreite allerdings sehr groß war und von einer sofortigen Rückmeldung der Unternehmen bis zu 68 Tagen reichte. Betrachtet man die Reaktionszeit nach Unternehmenstypen, lassen sich ebenfalls große Unterschiede feststellen. Mit durchschnittlich 2,5 Tagen reagierten die Globalen Distributionssysteme, gefolgt von Telekommunikationsunternehmen mit 8,4 Tagen, am schnellsten auf die Anfragen des BfV und BAMAD, während die Luftfahrtunternehmen mit 29 Tagen im Durchschnitt die längste Reaktionszeit hatten.
Daran wird deutlich, dass die gemäß § 8a Abs. 2 S. 1 Nr. 1 und 4 BVerfSchG zur Auskunft verpflichteten Unternehmen in der Regel recht schnell auf die Anfragen der Nachrichtendienste reagieren. Dies spiegelte sich auch in der Bewertung der Reaktionszeit durch die Nachrichtendienste wider. In mehr als 80 Prozent der Fälle meldeten sich die jeweiligen Unternehmen nach Bewertung der Nachrichtendienste schnell bzw. sehr schnell zurück. In sechs Prozent der Fälle wurde die Reaktionszeit als zufriedenstellend beurteilt. Hingegen wird das Antwortverhalten bei knapp 11 Prozent der Unternehmen als langsam bzw. sehr langsam eingestuft.

Abb. 3: Bewertung der Reaktionszeit der nach § 8 Abs. 2 S. 1 Nr. 1 und 4 BVerfSchG zur Auskunft verpflichteten Unternehmen durch BfV und BAMAD



Demgegenüber betrug die Reaktionszeit der gemäß § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG sowie des BZSt im Durchschnitt 17,1 Tage. Auch hier war die Spannbreite sehr groß und reichte von einem Tag bis zu 125 Tagen. Betrachtet man die Reaktionszeit etwas differenzierter, lassen sich ebenfalls große Unterschiede erkennen. Am schnellsten reagierte auf die Anfragen der Nachrichtendienste das BZSt, das im Durchschnitt 3,5 Tage für eine Rückmeldung benötigte, gefolgt von den Finanzunternehmen (15,3 Tage), den Kreditinstituten (17,7 Tage) und den Finanzdienstleistungsunternehmen (22,3 Tage).
Verglichen mit den Reaktionszeiten der Telekommunikationsdiensteanbieter sowie der Luftfahrtunternehmen und der Globalen Distributionssysteme fiel die Bewertung der für die Finanzermittlung relevanten Unternehmen schlechter aus. Dies ist vermutlich darauf zurückzuführen, dass die durchschnittliche Reaktionszeit fast doppelt lang war. So erfolgten in 60 Prozent der Fälle die Rückmeldungen der Unternehmen nach Bewertung der Nachrichtendienste schnell bzw. sehr schnell. In 27 Prozent der Fälle wurde die Reaktionszeit als zufriedenstellend beurteilt. Hingegen wurde das Antwortverhalten bei knapp 13 Prozent der Übermittlungen als langsam bzw. sehr langsam eingestuft.

Abb. 4: Bewertung der Reaktionszeit der nach § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG zur Auskunft verpflichteten Unternehmen sowie des BZSt durch BfV, BND und BAMAD



Probleme bei der Erteilung der Auskünfte

Bei der Erteilung der gewünschten Auskünfte gab es kaum Probleme. Lediglich bei drei Anordnungen des BND und BAMAD gab es Schwierigkeiten. In zwei Fällen traten – entgegen bisheriger Erfahrungen – mit einem Kreditinstitut „Verständnisprobleme“ auf. Seitens des Kreditinstituts wurde im Nachgang zu telefonischen Erläuterungen die Erforderlichkeit der Auskunftserteilung schriftlich hinterfragt, da weder schwerwiegende Gefahren noch die Annahme rechtfertigende Tatsachen ersichtlich gewesen seien. Die Bedenken konnten letztlich mit schriftlichen Hinweis auf den geheimen Sachverhalt und die zuständigen Prüf-/Anordnungsinstanz sowie die G 10-Kommission überwunden werden. In einem weiteren Fall war es zu Problemen gekommen, da dem BZSt von einem Nachrichtendienst zunächst ein falsches Geburtsdatum übermittelt worden war.

Lösch- und Benachrichtigungspflichten

Mit Blick auf die Lösch- und Benachrichtigungspflichten, die im neu eingefügten § 8b BVerfSchG zusammengefasst wurden, ist zu bemerken, dass es – bezogen auf die im Erhebungszeitraum abgeschlossenen Maßnahmen – in keinem Fall den Betroffenen mitgeteilt wurde, dass über sie gemäß § 8a Abs. 2 und 2a BVerfSchG Daten erhoben wurden. Vom für Finanzermittlungen zuständigen BfV-Fachreferat wurde als Hauptgrund für die bisher nicht erfolgte Mitteilung genannt, dass die Maßnahmen zum Zeitpunkt der Beantwortung des Fragebogens noch nicht abschließend ausgewertet gewesen seien und eine Mitteilung erst spätestens nach einem Jahr erfolgen müsse. Darüber hinaus wurden als Gründe genannt, dass der Vorgang noch nicht abgeschlossen gewesen sei und die Prüfung der Mitteilung noch ausstehe. In einem Fall begründete das Finanzreferat des BfV die nicht erfolgte Mitteilung damit, dass die Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden könne. Das für die Abfrage von Daten bei Telekommunikationsdiensteanbietern zuständige Fachreferat gab als Hauptgrund an, dass aufgrund der erst kürzlich erfolgten Beendigung der Maßnahme eine Entscheidung über die Unterrichtung der Betroffenen noch ausstehe. Des Weiteren wurde die nicht erfolgte Mitteilung damit begründet, dass es sich um eine fiktive/ unbekannte Personalie handele.

Der BND begründete seine Entscheidung damit, dass der Sachverhalt derzeit noch in Bearbeitung sei und weitere Auskünfte noch ausstehen würden bzw. die Mitteilung noch geprüft werde.

Das BAMAD gab als Gründe für die nicht erfolgte Mitteilung an, dass die Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden könne und andere Erhebungsformen geheimhaltungsbedürftig seien. Darüber hinaus wurde darauf hingewiesen, dass die besonderen Auskunftsersuchen als ein Bestandteil – neben anderen – der nachrichtendienstlichen Fallbearbeitung ergänzend durchgeführt werden. Die Frage und Entscheidung über die Mitteilung an den Betroffenen könne nur in Zusammenhang mit der etwaigen Mitteilung anderer Maßnahmen getroffen werden.

Zudem wurden auch keine im Erhebungszeitraum gemäß § 8a Abs. 2 und 2a BVerfSchG, § 4a MADG und § 3 BNDG erhobenen Daten gelöscht. Das für Finanzermittlungen zuständige Fachreferat des BfV begründete dies hauptsächlich damit, dass nach § 8b Abs. 2 BVerfSchG eine analoge Anwendung von § 4 G 10 für die erhobenen Daten maßgeblich sei. Danach prüfe der zuständige Fachbereich halbjährlich, ob die Daten noch benötigt würden. Allerdings könne das Finanzermittlungsreferat die erhobenen Daten erst ein Jahr nach Mitteilung an den Betroffenen löschen/vernichten. Bis zu diesem Datum müsse es alle Unterlagen sowie erhobene Daten für den Betroffenen zu Beweiszwecken in einem eventuellen Klageverfahren bereithalten. Als weiterer Grund wurde vom Finanzermittlungsreferat des BfV angegeben, dass der Vorgang noch nicht abgeschlossen sei. Des Weiteren gab das für die Datenabfrage bei den Telekommunikationsdiensteanbietern zuständige Fachreferat des BfV an, dass aufgrund der erst kürzlich erfolgten Beendigung noch keine Daten gelöscht worden seien.

Das BAMAD wies in zwei Fällen darauf hin, dass die Auswertung der Daten noch nicht abgeschlossen sei. Als weiterer Grund für die Beibehaltung der erhobenen Daten wurde angeführt, dass diese noch erforderlich seien, um sie mit anderen neuen nachrichtendienstlichen Informationen in einen Kontext setzen zu können.

Der BND gab an, dass in einem Fall die Mitteilungsentscheidung noch zu prüfen sei. Falls es zu einer Mitteilung kommen sollte, müssten die Daten noch bis zum Ablauf der Frist einer möglichen gerichtlichen Überprüfung zugriffsgesperrt aufbewahrt werden. Erst danach könne die Löschung erfolgen. In zwei Fällen wurde die Beibehaltung der Daten damit begründet,

dass ein Folgeantrag, mit dem Auskünfte von zahlreichen weiteren Kreditinstituten angefordert worden seien, noch in Bearbeitung sei.

Mitteilungsverfahren gemäß § 8b Abs. 7 BVerfSchG (2015-2017)

Da zu den Maßnahmen, die zwischen dem 1. Oktober 2016 und dem 30. September 2017 abgeschlossen und übermittelt wurden, noch keine Entscheidung vorlag, ob die Betroffenen hierüber unterrichtet werden können oder nicht, wurden die drei Nachrichtendienste darum gebeten, Informationen zu Mitteilungsprüfungen für den Zeitraum 1. Januar 2015 bis 31. Dezember 2017[107] zur Verfügung zu stellen. Hierbei handelte es sich um evaluierungspflichtige Maßnahmen gemäß § 8a Abs. 2 und 2a BVerfSchG, die nicht im Erhebungszeitraum abgeschlossen worden waren. Diese zusätzlichen Informationen sollten dazu dienen, einen besseren Eindruck zu bekommen, wie sich die Mitteilungspraxis bei den drei Nachrichtendiensten darstellt.

BfV

Die Mitteilungsprüfung beim BfV läuft wie folgt ab: Nach Beendigung einer Beschränkungsmaßnahme wird der Bedarfsträger aufgefordert, zu der Frage Stellung zu nehmen, ob eine Mitteilung an den Betroffenen erfolgen kann (§ 12 Abs. 1 G 10). Dabei werden auch die LfV, soweit diese mit dem Fall befasst waren oder sind, eingebunden (sog. Benehmensherstellung). Aufgrund der Stellungnahmen des Bedarfsträgers und ggf. der externen Behörden unterbreitet die G10-Stelle/das Finanzermittlungsreferat dem BMI einen entsprechenden Mitteilungsvorschlag. Nach der Entscheidung der G 10-Kommission über die vorgelegten Mitteilungsvorschläge ergeht ein entsprechender Erlass des BMI. Aufgrund dessen wird im Mitteilungsfall der Bedarfsträger durch das BfV zeitnah unterrichtet und eine Anschriftenabklärung zu den Betroffenen durchgeführt. Die Mitteilung an den Betroffenen erfolgt grundsätzlich durch Bescheid per Postzustellungsurkunde. Teilweise haben sich die Betroffenen telefonisch oder schriftlich beim BfV gemeldet und Nachfragen gestellt, um weitere Erläuterungen zu der Beschränkungsmaßnahme zu erhalten. In einem Fall erhob ein Betroffener Klage.
Neben den Mitteilungen zu den im Erhebungszeitraum abgeschlossenen Maßnahmen (s. o.) wurden die Nachrichtendienste zu den im Zeitraum Januar 2015 bis Juni 2017 durchgeführten Mitteilungsüberprüfungen befragt. Hier verliefen die Mitteilungsüberprüfungen des BfV zu 83 Maßnahmen nach § 8a Abs. 2 BVerfSchG zu 168 Betroffenen (101 Haupt- und 67 Nebenbetroffene) positiv. Dagegen unterblieb in zwei Fällen[108] (zwei Haupt- und drei Nebenbetroffene) eine Mitteilung, obschon die rechtlichen Voraussetzungen gegeben waren. Als Gründe für die Nichtmitteilung wurden genannt, dass eine aktuelle Anschrift nicht ermittelt werden konnte, die Betroffenen unter einem Aliasnamen bzw. einer Fiktivpersonalie aktiv waren und die wahre Identität nicht bekannt ist.
Zwischen Januar 2015 und Juni 2017 ergab die Prüfung des BfV von 173 Maßnahmen, dass die Mitteilung an 329 Betroffene (221 Haupt- und 108 Nebenbetroffene) zurückgestellt wurde. Begründet wurde die Zurückstellung seitens des BfV damit, dass bei einer Mitteilung eine Gefährdung des Zwecks der Beschränkungsmaßnahme nicht ausgeschlossen werden konnte (z. B. weil der Betroffene weiterhin im Visier nachrichtendienstlicher Sachverhaltsermittlung stand) und/oder der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar war (z. B. weil so Rückschlüsse auf die Arbeitsweise eines Nachrichtendienstes hätten gezogen werden können oder in absehbarer Zeit die Wiederaufnahme einer

[107] Das BfV konnte aus organisatorischen Gründen nur Informationen für den Zeitraum 1. Januar 2015 bis 30. Juni 2017 zur Verfügung stellen.
[108] Eine Auskunft war hier nur für das 1. Halbjahr 2017 möglich.

entsprechenden Überwachung wahrscheinlich oder nicht ausgeschlossen erschien). Die G 10-Kommission gab dem Antrag auf Zurückstellung, die in der Regel für zwei Jahre, teilweise aber auch für einen kürzeren Zeitraum erfolgte, in allen Fällen statt.
Sofern Bedenken gegen eine Mitteilung an einen Betroffenen bestehen, muss ausführlich begründet werden, dass eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist (vgl. § 12 Abs. 1 G 10). Das ist vor allem der Fall, wenn der Verdacht im Sinne der § 1 Abs. 1 Nr. 1, § 3 Abs. 1 G 10 gegen den Betroffenen fortbesteht, eine weitere Beschränkungsmaßnahme gegen ihn/sie läuft oder wenn aufgrund der Mitteilung Belange des Verfassungsschutzes oder anderer Sicherheitsbehörden beeinträchtigt werden könnten. Hierbei sind mögliche personelle Verflechtungen zwischen den Betroffenen zu prüfen und darzulegen, aus welchem Grund die Nichtmitteilung gegenüber einem Betroffenen der positiven Mitteilung an andere Betroffene der gleichen Maßnahme nicht entgegensteht (z. B. da kein Kennverhältnis zwischen den Personen besteht).
In 16 Fällen, bei denen es um 102 Haupt- und 88 Nebenbetroffene ging, stimmte die G 10-Kommission einer endgültigen Nichtmitteilung zu. In diesen Fällen wurde festgestellt, dass auch fünf Jahre nach Beendigung der Maßnahme noch eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden konnte und/oder der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar war und mit an Sicherheit grenzender Wahrscheinlichkeit auch in der Zukunft vorliegt und die Voraussetzungen für eine Löschung sowohl bei der erhebenden Stelle als auch beim Empfänger vorliegen.

BAMAD

Beim BAMAD läuft das Verfahren wie folgt ab: Nach der Entscheidung über die Mitteilung der G 10-Kommission und der Aktualisierung der Wohnadressen/Aufenthaltsorte der Betroffenen durch den jeweiligen Fachbereich werden die Mitteilungsbescheide durch das G 10-Dezernat erstellt. Nach Billigung der Mitteilungsbescheide sowie des beabsichtigten weiteren Vorgehens durch die Amtsführung werden die Bescheide mit Postzustellungsurkunde verschickt. Ggf. erfolgt eine Terminvereinbarung mit den Betroffenen zwecks persönlicher Zustellung gegen Empfangsbekenntnis. Nach erfolgter Zustellung werden Kopien der Reinschriften der Bescheide sowie der ausgefertigten Postzustellungsurkunden bzw. der Empfangsbekenntnisse an das BMI übersandt. Für den Fall, dass mehrere Personen von einer Maßnahme betroffen sind, jedoch die Benachrichtigung an eine dieser Personen zurückgestellt und ausgeschlossen werden soll, werden die Mitteilungsentscheidungen für jeden Betroffenen nach Einzelfallbewertung getrennt getroffen. Die Mitteilungsentscheidungen und die Nichtmitteilungsentscheidungen werden dann gebündelt und jeweils getrennt der G 10-Kommission präsentiert. Vorrang hat dabei der Teil der Entscheidungen, bei denen es um die Mitteilung geht, damit diese unverzüglich erfolgen kann.
Die Betroffenen reagierten nach Angaben des BAMAD unterschiedlich auf die Mitteilung, dass eine Anordnung gemäß § 4a MADG i. V. m. § 8a BVerfSchG gegen sie gerichtet war. Das Spektrum reichte dabei von Erleichterung, über Erstaunen, Gefasstheit, keiner Reaktion bis hin zu Wut. Zu Klageverfahren ist es dagegen nicht gekommen.
In einem Fall teilte das BAMAD zwei Betroffenen (einem Haupt- und einem Nebenbetroffenen) mit, dass eine Anordnung gemäß § 4a MADG i. V. m. § 8a BVerfSchG gegen sie gerichtet war. In vier Fällen wurde eine Mitteilung zurückgestellt, die mit Quellenschutz, der Gefährdung operativer Belange des BAMAD und laufender Ermittlungen anderer Sicherheitsbehörden, der ernsthaften Beeinträchtigung laufender operativer Maßnahmen einer Verfassungsschutzbehörde sowie einer Strafverfolgungsbehörde begründet wurde. Hierbei handelte es sich um

vier Haupt- und drei Nebenbetroffene. In drei Fällen stimmte die G 10-Kommission der Zurückstellung der Mitteilung für zwei Jahre und in einem Fall für neun Monate zu. Im Erhebungszeitraum wurde kein Antrag des BAMAD auf Zurückstellung von der G 10-Kommission abgelehnt.

BND

Der BND verwies darauf, dass es sich bei den Betroffenen überwiegend um Ausländer im Ausland handele, zu denen der BND weder ihre Erreichbarkeit noch die Betroffenen recherchieren könne, ohne diese dadurch möglicherweise zu gefährden. In den Eigensicherungsfällen gebe es bei der nachträglichen Mitteilung an die Betroffenen, also hauptamtliche Mitarbeiter des BND, keine Probleme. Die Mitteilung erfolge fallabhängig schriftlich per Postzustellungsurkunde oder durch persönliche Übergabe des Mitteilungsschreibens. In den übrigen Fällen scheide die Mitteilung aus o. g. Gründen in der Regel faktisch aus. Aus Sicht des BND sei diese zudem widersprüchlich, da sie als Schutz für den Betroffenen gedacht sei, aber in Auslandsfällen eine Mitteilung oft mit erheblicher persönlicher Gefährdung des Betroffenen verbunden sei. Im Zeitraum 1. Januar 2015 bis 31. Dezember 2017 hat es weder einen Mitteilungsfall noch einen Fall auf Zurückstellung beim BND gegeben.

4.2.2.4. Bewertung und Optimierungsbedarf aus Sicht der Nachrichtendienste

Das Nutzungsverhalten der Nachrichtendienste hinsichtlich der besonderen Auskunftsverlangen fällt sehr unterschiedlich aus. Bislang nutzte in erster Linie das BfV die Befugnisse, während BND und BAMAD nur in wenigen Fällen darauf zurückgriffen. Dies lag vor allem daran, dass beim BND aufgrund des Auslandsbezugs der Tätigkeit sowie beim BAMAD aufgrund der Beschränkung der Zuständigkeit auf den Geschäftsbereich des BMVg die Instrumente eher selten zum Einsatz kommen können.
Dennoch betonten alle drei Nachrichtendienste, dass die besonderen Auskunftsverlangen ein wichtiges und wertvolles Instrument für die nachrichtendienstliche Arbeit seien. Nach Einschätzung des BfV und BAMAD sei die Abfragemöglichkeit bei Telediensteanbietern (Bestandsdaten) sehr nützlich, da mit ihr Informationen für weitere Ermittlungen gewonnenen werden könnten. Zudem könnten die dort erhaltenen Daten zur Verdichtung bereits vorhandener Informationen genutzt werden. Laut BfV sei der erhebliche Anstieg der Fallzahlen v. a. in der geänderten Sicherheitslage, aber auch in den erst zwischenzeitlich etablierten Arbeitsabläufen zu erklären. Der BND gab an, dass die neu geschaffene Möglichkeit, Bestandsdaten von Telediensteanbietern zum Zwecke der Eigensicherung zu erheben, nützlich sei und als wichtige Erweiterung angesehen werde. Darüber seien weitere Einsatzmöglichkeiten denkbar (z. B. im Bereich Internet-Drogenhandel, Bestellung von Dual-Use-Gütern (z. B. Wasserstoffperoxid) über Internet-Versandhändler). Das BAMAD und der BND wiesen zudem darauf hin, dass das Verfahren nicht so komplex sei bzw. es keine zu hohen Verfahrensanforderungen gebe.
Mittlerweile gebe es mit dem sog. Passenger Name Record (PNR) eine weitere Möglichkeit für die Sicherheitsbehörden, Fluggastdaten zu erhalten, wobei die diesbezüglichen rechtlichen Anforderungen geringer als im BVerfSchG seien. Daher stelle sich hier die Frage, wie sich die Befugnisse zueinander verhielten. Das BfV plädierte hier für eine Anpassung der gesetzlichen Anforderungen im § 8a Abs. 2 Nr. 1 BVerfSchG an die des PNR.
Die Ausdehnung der Befugnisse gemäß § 8a Abs. 2 S. 1 Nr. 1 BVerfSchG auf Computerreservierungssysteme und Globale Distributionssysteme ermögliche es, Auskünfte zu Reiserouten einzuholen, falls nicht bekannt sei, welche Fluggesellschaft genutzt werde bzw. es sich um eine ausländische Fluggesellschaft handele, die nicht kontaktiert werden solle, da sie

Verbindungen zu den Sicherheitsbehörden des jeweiligen Landes (von dem z. B. die aufzuklärende Spionageaktivität ggf. ausgeht) unterhalte. Zudem könne man über diese Systeme z. T. Informationen erhalten, die man von den Fluggesellschaften nicht bekommen hätte. Als nachteilig wurde es von BfV und BAMAD angesehen, dass für Anfragen an Computerreservierungssysteme sehr konkrete Angaben (z. B. zu Start- und Zielflughafen, Zwischenstopps) erforderlich seien, die im Vorhinein oft schwer zu ermitteln seien.
Durch die Schaffung der Möglichkeit, Auskünfte beim BZSt einzuholen, habe sich die Abfrage von Kontostammdaten deutlich vereinfacht, da nicht alle Kreditinstitute einzeln angeschrieben werden müssten, um die gewünschten Informationen zu erhalten. Über die Kontostammdatenauskunft erhalte man eine Übersicht über alle Konten eines Betroffenen und die Konten, über die er bevollmächtigt ist. Dies ermögliche nach anschließender Kontoauskunft einen Gesamtüberblick über die finanzielle Situation des Betroffenen. Zudem erhalte man über die Kontostammdaten weitere berechtigte Personen (z. B. Firmenmitinhaber), die über die Konten des Betroffenen Vollmacht besitzen.
Das BfV wies im Übrigen im Zusammenhang mit der Kontostammdatenauskunft über das BZSt darauf hin, dass hier ein aufwändiges G 10-Verfahren dazu führe, dass erst sehr spät festgestellt werde, dass relevante Konten weiterer Personen vorlägen, deren Beauskunftung dann erst mittels eines Erweiterungsantrages in der G10-Kommission beantragt werden könnten. Dies wiederum sei aufwändig und koste v. a. bei Gefährdungslagen wertvolle zusätzliche Zeit. Das BfV halte bei der Kontostammdatenauskunft über das BZSt zudem eine Reverssuche für erforderlich, welche z. B. dem BKA nach § 24c KWG bei der BaFin bereits zur Verfügung stünde.
Das Instrument der Finanzermittlung hat nach Angabe des BfV deutlich an Aussagekraft gewonnen, da nun eine breite und verlässliche Datenbasis für Strukturauswertungen zur Verfügung stehe, um Finanzflüsse zwischen Beteiligten und ihre Funktionen und Stellungen in Netzwerken besser erkennen zu können.
Als vorteilhaft wurde auch die Möglichkeit gesehen, im Rahmen eines Kombi-Antrags die Kontostammdatenabfrage mit der Erlaubnis zur Überprüfung der vom BZSt mitgeteilten Konten zu verknüpfen, was zu einer deutlichen Vereinfachung und Beschleunigung des Arbeitsablaufs geführt habe, da v. a. nur ein G 10-Verfahren erforderlich sei. Dies gelte allerdings nur für das BfV und das BAMAD. Der BND nutze einen Kombi-Antrag grundsätzlich nur bei bereits bekannten Parametern, z. B. einem bekannten Konto. Die Abfragemöglichkeit bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen sei ein wichtiges und unverzichtbares Instrument, um Informationen zu finanziellen Unterstützungstätigkeiten von terroristischen Organisationen im Ausland, zu Finanzströmen im rechts- und linksextremistischen Kontext oder im Zusammenhang mit Proliferation oder Spionagetätigkeiten zu erhalten. Die hierbei gewonnenen Erkenntnisse könnten zudem in G 10-Maßnahmen einfließen.
Mit der Abfrage von Verkehrsdaten bei Telekommunikationsunternehmen könnten wertvolle Informationen zum Kommunikationsverhalten und Umfeld bzw. zu Netzwerken einer Zielperson gewonnen werden. Von Vorteil sei dabei, dass die Verkehrsdaten sowohl rückwirkend als auch für die Zukunft abgefragt werden können. Zudem handele es sich um – im Vergleich zur Inhaltsüberwachung – weniger eingriffsintensive Maßnahmen. Auf Grundlage der hier gewonnenen Erkenntnisse ließen sich G 10-Maßnahmen besser und gezielter vorbereiten.
Die Befugnis zur Abfrage von Teledienstverkehrsdaten sei nach Ansicht der drei Nachrichtendienste ebenfalls ein wichtiges nachrichtendienstliches Instrument, um z. B. Chatverläufe nachvollziehen zu können. Bislang wurden jedoch kaum Erfahrungen in diesem Bereich gesammelt.

Als Hauptnutzer der Befugnisse nach §§ 8a-c BVerfSchG wurde insbesondere vom BfV, jedoch auch vom BND und BAMAD, in verschiedenen Bereichen Optimierungsbedarf festgestellt. Zum einen wurde sowohl von Seiten des BfV als auch von Seiten des BAMAD die Wiedereinführung der Befugnisse zu Auskunftsverlangen gegenüber Postdienstleistern gefordert, da es Fälle in der Vergangenheit gegeben habe, in denen im rechtsextremistischen Bereich eine konspirative Netzwerkkommunikation über Postfächer zwischen verschiedenen Haftanstalten stattgefunden habe. Darüber hinaus würden auch heute rechtsextreme Labels und Vertriebe mit Postfächern und Paketstationen operieren. Im Bereich Islamismus und Linksextremismus würden ebenfalls Informationen über Briefe und Postfächer ausgetauscht. Eine solche Abfrage ermögliche es den Nachrichtendiensten herauszufinden, wem ein Postfach gehört bzw. wer Zugriff darauf hat.
Zu § 8a Abs. 1 BVerfSchG merkte das BfV an, dass die Anforderungen an die Maßnahme – verglichen mit der Abfrage nach TKG – sehr hoch seien. So werde das dem BVerfSchG, dem G 10 und auch der Rechtsprechung des BVerfG zugrundliegende Verhältnismäßigkeitsprinzip zwischen der Intensität des Grundrechtseingriffs und den Rechtfertigungsvoraussetzungen atypisch durchbrochen. Durch das Änderungsgesetz aus dem Jahr 2011 wurde festgelegt, dass auch Auskunftsverlangen zu Bestandsdaten bei Teledienstanbietern grundsätzlich mitteilungspflichtig sind, da § 8b Abs. 7 BVerfSchG auch für Auskünfte nach § 8a Abs. 1 BVerfSchG gilt. Zuvor gab es eine solche Pflicht im BVerfSchG nicht. Zudem sind Bestandsdatenauskünfte zu Telekommunikationsdiensten gemäß § 8d Abs. 1 BVerfSchG nach wie vor nicht mitteilungspflichtig. Auch muss gemäß § 8b Abs. 7 BVerfSchG i. V. m. § 12 Abs. 1 S. 3 G 10 nun sogar noch die G 10-Kommission über die hier vorliegenden Einzelfälle entscheiden, deren Zurückstellung länger als 12 Monate andauert. Dies verursache einen unnötigen Aufwand. Daher sollte nach Auffassung des BfV und des BAMAD auf eine Mitteilungspflicht bei der Bestandsdatenabfrage bei Teledienstanbietern verzichtet werden. Zumindest sollte jedoch davon abgesehen werden, die Entscheidung über die längerfristige Zurückstellung und die endgültige Nichtmitteilung von der G 10-Kommission treffen zu lassen. Der BND wies in diesem Kontext darauf hin, dass Wortlaut und Systematik des § 12 Abs. 2 G 10 überdehnt würden, wenn an das Vorliegen einer Zweckgefährdung für eine endgültige Nicht-Mitteilung strengere Anforderungen gestellt würden als an eine Zurückstellung.[109]
Aufgrund der Tatsache, dass es bei ausländischen Unternehmen keine Möglichkeit gebe, diese zur Auskunftserteilung zu verpflichten, plädierten das BfV und das BAMAD für die Einführung des „Marktortprinzips“. Dadurch müssten sich ausländische Unternehmen, die eine Dienstleistung in Deutschland anbieten, den deutschen Sicherheitsgesetzen unterwerfen. Zudem wurde von beiden Nachrichtendiensten moniert, dass in § 8a Abs. 1 BVerfSchG immer noch auf das „alte“ TDG verwiesen werde. Hier sollte eine Anpassung des Verweises auf das aktuelle TMG erfolgen, da es sich bei den Telediensten um einen veralteten Rechtsbegriff handele.
Ein Problem stelle derzeit auch noch die Behandlung von Over-the-top-Playern (z. B. WhatsApp) dar, da für jede Funktionalität zu prüfen sei, ob es sich um Teledienste oder TK-Dienste handelt, weshalb man im Einzelfall nicht immer sicher sei, welche Ermächtigungsgrundlage für Maßnahmen im Zusammenhang mit dieser verbreiteten Kommunikationsform greife.
Des Weiteren solle die Eingriffsschwelle für Abfragen gemäß § 8a Abs. 1 BVerfSchG abgesenkt werden. Das BfV plädierte zudem für die Einführung einer Verifikationspflicht für Nutzer von Telediensten, damit die besonderen Auskunftsverlangen nicht ins Leere laufen.

[109] Die Ausführungen zur Bedeutung des G 10 im Kontext der Mitteilungspflicht gelten entsprechend für alle besonderen Auskunftsverlangen und IMSI-Catcher.

Schließlich wäre es wünschenswert, wenn der Datenkranz der zu übermittelnden Informationen und das Format für die Teledienstbestandsdaten gesetzlich festgelegt würden.
Insgesamt sei eine Anpassung an die Vorgaben zur Bestandsdatenabfrage im TKG-Bereich (§ 113 TKG) wünschenswert. Mit Blick auf die besonderen Auskunftsverlangen gemäß § 8a Abs. 2 S. 1 Nr. 1 BVerfSchG regte das BfV und das BAMAD an, auf das G 10-Antragsverfahren zu verzichten oder zumindest die Möglichkeit einer endgültigen Nichtmitteilung zu schaffen, da dieses sehr zeitaufwendig sei und Ressourcen binde. Zudem sei es nicht erforderlich, da es sich nicht um einen Eingriff in Art. 10 GG handele. Darüber hinaus wurde vom BfV Optimierungsbedarf bei der Zusammenarbeit mit den zur Auskunft verpflichteten Unternehmen gesehen. So sollte klar festgelegt werden, welcher Datenkranz von den Unternehmen zur Verfügung gestellt sowie in welchem Format und auf welchem Weg die Daten an BfV übermittelt werden müssen.
Zu § 8a Abs. 2 S. 1 Nr. 2 und Abs. 2a BVerfSchG wurde ebenfalls auf das aufwendige Antragsverfahren sowie die Probleme bei der Mitteilungspflicht hingewiesen. Auch hier liege kein Eingriff in Art. 10 GG vor, sodass die Einbeziehung der G 10-Kommission eigentlich nicht erforderlich sei. Bei der Erhebung von Kontostammdaten handele es sich im Vergleich zur Erhebung von Verkehrs- und Inhaltsdaten ebenfalls um eine Maßnahme mit geringer Eingriffsintensität. Dies rechtfertige eine Differenzierung im Hinblick auf die Erhebungsvoraussetzungen und Verfahrensvorschriften, mithin einen Verzicht auf das G 10-Verfahren für die Kontostammdatenauskünfte. Dies würde der normativen Differenzierung nach dem Eingriffsgehalt einer Maßnahme sowie der Gesetzeswertung und -systematik im (vergleichbaren) Bereich der Auskunftsersuchen zu Telekommunikationsbestandsdaten nach §§ 112, 113 TKG entsprechen. Im Sinne der o. g. Differenzierung solle zudem eine Regelung geschaffen werden, wonach eine Mitteilungspflicht (entsprechend Auskunftsersuchen zu Bestandsdaten von Telekommunikationsdiensten) bei Kontostammdatenauskünften entfällt.
Die fehlende Möglichkeit einer endgültigen Nichtmitteilung führe dazu, dass immer wieder geprüft und entschieden werden müsse, ob mitgeteilt werden könne oder nicht. Zudem bestehe ein dauerhafter Widerspruch, wenn bei einer parallel durchgeführten G 10-Maßnahme endgültig entschieden werde, auf eine Mitteilung zu verzichten. Des Weiteren sei es aus Sicht des BfV und BAMAD wünschenswert, wenn auch die ausländischen Finanzunternehmen – neben den bereits oben genannten Telediensteanbietern – durch die Einführung des „Marktortprinzips“ dazu verpflichtet würden, Auskünfte zu erteilen. Das BfV wies in diesem Zusammenhang auf das Problem einer Auskunftseinholung bei europäischen oder internationalen Unternehmen der Finanzbranche hin, die z. B. mit ihrer europäischen Lizenz ihre Bank- und Transferdienstleistungen auch in Deutschland anbieten könnten, aber nicht dem deutschen Recht unterlägen und daher auch nicht der Aufsicht der BaFin unterstünden. Aus Sicht des BfV sei es erforderlich, eine rechtliche Grundlage im Hinblick auf ausländische Anbieter zu schaffen, um eine wirksame rechtliche Handhabe für die Auskunftserteilung durch ausländische Anbieter zu erhalten. Zudem müsse das Benachteiligungsverbot effektiv durchgesetzt werden können, indem durch eine gesetzliche Klarstellung den zur Auskunft verpflichteten Unternehmen deutlich gemacht würde, dass ein Auskunftsverlangen der Nachrichtendienste nicht die Verpflichtung zur Abgabe eine Geldwäscheverdachtsmeldung auslöse. Ein weiteres Problem ergebe sich daraus, dass die zur Auskunft verpflichteten Unternehmen – teilweise unter Berufung auf § 3 Abs. 1 NDÜV – die Daten in sehr unterschiedlichen Formaten übermittelten (z. B. Papier, PDF, DVD, E-Mail, teils mit Link und Passwort). Dies habe zur Folge, dass die Daten teilweise immer noch händisch bearbeitet und ausgewertet werden müssten.

Sowohl BfV als auch BND hielten es für diskussionswürdig, ob bei der Einholung von Kontostammdaten das gleiche Schutzniveau wie bei der Einholung von Verkehrsdaten im Telekommunikationsbereich zugrunde gelegt werden müsse.
Zu § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG wurde ebenfalls auf das aufwendige G 10-Antragsverfahren sowie die Mitteilungsproblematik hingewiesen. Mit Blick auf die für effektive Aufklärungsarbeit wünschenswerte rückwirkende Abfrage von Telekommunikationsverkehrsdaten sei eine Regelung zur Vorratsdatenspeicherung sinnvoll. Diese sollte die Nachrichtendienste explizit als berechtigte Abfragestellen benennen, da es immer wieder Hinweise von ausländischen Nachrichtendiensten zu TK-Verbindungen aus der Vergangenheit gebe. In diesem Zusammenhang solle eine praxistaugliche Speicherfrist und ein angemessener Datenkranz an vorzuhaltenden Informationen (z. B. IP- und Portnummer) festgelegt werden.
Mit Blick auf die Möglichkeit, gemäß § 8a Abs. 2 S. Nr. 5 BVerfSchG Teledienstverkehrsdaten abzufragen, verwies das BfV auf das Problem der Verweisung auf das alte, nicht mehr gültige TDG. Hier sollte – wie bei den Bestandsdaten – der Verweis auf das aktuelle TMG erfolgen. Zudem sei zu überlegen, ob die Nummern 4 und 5 nicht zusammengefasst werden, da auf EU-Ebene von sog. konvergenten Diensten gesprochen werde, die sich der klassischen Unterscheidung von TK- und Telediensten entziehen würden. Zudem würde eine Zusammenlegung auch die Wahrscheinlichkeit für die Schaffung eines gemeinsamen Formats erhöhen.

4.2.3. Rechtswissenschaftliche Bewertung

4.2.3.1. § 8a BVerfSchG

Bestandsdatenauskunft nach § 8a Abs. 1 BVerfSchG

Die Bestandsdatenauskunft nach § 8a Abs. 1 BVerfSchG stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.[110] Hinsichtlich der Geeignetheit der Maßnahmen zum Schutz der in § 3 Abs. 1 BVerfSchG genannten Rechtsgüter gibt die empirische Analyse keinen Anlass zu Zweifeln. Ein gleich wirksames milderes Mittel ist nicht erkennbar. Die Fallzahlen sind gegenüber dem letzten Berichtszeitraum erheblich gestiegen. Dies lässt für sich noch keinen Hinweis auf eine fehlende Angemessenheit zu, da sich das Nutzungsverhalten potenziell Betroffener in den letzten Jahren hin zu sog. sozialen Netzwerken (hier namentlich Facebook) entwickelt und sich die Sicherheitslage verschärft hat. Zudem hätten sich laut BfV die internen Abläufe zunächst etablieren müssen, um das Instrument zielgerichtet einsetzen zu können. Ein Anstieg der entsprechenden Befugnisse war deshalb durchaus naheliegend. Auch indiziert das Gesamtniveau mit gut 20 Auskunftsersuchen pro Monat keinesfalls eine flächendeckende Nutzung ohne angemessene Einzelfallprüfung. Hier ist auch auf den begrenzten Personenkreis der Beantragungsbefugten hinzuweisen, der insoweit eine gewisse verfahrensmäßige Vorkehrung für die Einzelfallprüfung trifft.
Dies gilt auch vor dem Hintergrund, dass den Nachrichtendiensten Zwangsmittel zur Durchsetzung des Auskunftsverlangens nicht zur Verfügung stehen, sie den Datenrückfluss also nicht beherrschen können.

Auskunftsverlangen nach § 8a Abs. 2 und 2a BVerfSchG

Die relativ geringe Zahl der besonderen Auskunftsverlangen nach § 8a Abs. 2 und Abs. 2a BVerfSchG weist auf eine insoweit zurückhaltende und das Gebot der Verhältnismäßigkeit im engeren Sinne beachtende Anwendungspraxis hin. Anhaltspunkte, die die Geeignetheit oder

[110] Vgl. BVerfG, NJW 2012, 1419 (1422); OVG Münster MMR 2002, 563 (564); Büttgen, in: Scheurle/Mayen, TKG (2008), § 96 Rn. 5. Differenzierend Gusy, in: von Mangoldt/Klein/Starck, GG (2010), Art. 10 Rn. 45.

Erforderlichkeit der von den Nachrichtendiensten auf der Grundlage dieser Vorschriften ergriffenen Maßnahmen zur Abwehr von Gefahren für die in § 3 Abs. 1 BVerfSchG genannten Schutzgüter in Frage stellen, ergeben sich aus der empirischen Erhebung nicht.
Ob die kumulative Abfrage bei Betreibern von Computerreservierungssystemen und Fluggesellschaften einen vertieften Grundrechtseingriff darstellt[111], kann hier dahinstehen, da es im Berichtszeitraum nur einen solchen Fall gab und sich dieses Mittel also als absolute Ausnahme darstellt. Ohne den Einzelfall beurteilen zu können, stellt sich jedenfalls die Anwendungspraxis insgesamt nicht als verfassungsrechtlich bedenklich dar.
In Anbetracht dessen, dass § 8a Abs. 2 und Abs. 2a BVerfSchG zu einer Reihe von Auskunftsverlangen ermächtigen, die allgemeine Nutzung von Telediensten zugenommen und die allgemeine Sicherheitslage sich verschärft hat, ist die Zahl der durch alle Nachrichtendienste des Bundes insgesamt nach diesen Vorschriften erhobenen Auskunftsverlangen mit 321 Anordnungen (inkl. den Bestandsdatenauskünften Teledienste, s. o.) in einem Jahr nicht sehr hoch, was auf einen zurückhaltenden Rückgriff auf diese Maßnahmen schließen lässt. Die Zahl der Nebenbetroffenen nach § 8a Abs. 3 Nr. 2 BVerfSchG liegt mit 29 deutlich unter der der Hauptbetroffenen (81) im Sinne von § 8a Abs. 3 Nr. 1 BVerfSchG.[112] Dies deutet ebenfalls darauf hin, dass die Nachrichtendienste besondere Auskunftsverlangen zurückhaltend handhaben und im Verhältnis zum Ziel der Maßnahme unverhältnismäßige, gleichsam flächenhafte Auskunftsverlangen nicht erfolgen.[113]

4.2.3.2. § 8b BVerfSchG

Da es im Erhebungszeitraum wegen der Notwendigkeit, die seitens der Nachrichtendienste durch Anordnungen nach § 8 Abs. 2 und 2a BVerfSchG erhobenen Informationen zur Auswertung bzw. zur Dokumentation für eventuelle gerichtliche Verfahren noch vorzuhalten, zu keiner Löschung von Daten gekommen ist, ist eine verfassungsrechtliche Bewertung der Praxis der Anwendung von § 8b Abs. 2 S. 7 BVerfSchG nicht möglich.
Die Mitteilung an Betroffene nach § 8b Abs. 7 BVerfSchG ist seitens der Nachrichtendienste in beträchtlichem Umfang erfolgt. Das Unterbleiben einer Mitteilung bedarf in jedem Einzelfall einer besonderen Begründung des Bestehens einer Gefährdung des Zwecks der Maßnahme oder des Eintritts übergreifender Nachteile für das Wohl des Bundes oder eines Landes. Verfassungswidrige Verkürzungen der Rechte der Betroffenen können daher nicht festgestellt werden.
Entsprechendes gilt für die Beurteilung der an die G 10-Kommission gerichteten Anträge auf Zurückstellung der Mitteilung. Das Kontrollsystem hat sich insoweit bewährt. Dass die Kommission derartige Anträge in der Vergangenheit jedoch auch abgelehnt hat, belegt das Funktionieren dieser Sicherung durch Verfahren.

---

[111] Vgl. Wolff/Mundil, ZG 2012, 278 (288 f.); Wolff, Stellungnahme, Innenausschuss, Drs. 17(4)359 B, S. 4; Schaar, Stellungnahme, Innenausschuss, Drs. 17(4)359 C, S. 10; Kugelmann, Stellungnahme, Innenausschuss, Drs. 17(4)359 F, S. 2. A.A. Eisvogel, Innenausschuss, Protokoll 17/52, S. 23. Differenzierend Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011, S. 58, wonach der vertiefte Grundrechtseingriff nicht gegenüber dem Betroffenen selbst gilt.
[112] Nicht erfasst werden konnten die Betroffenen zu § 8a Abs. 1 BVerfSchG, vgl. Kapitel 4.2.2.2.
[113] Zur Notwendigkeit der Unterlassung anlassloser Routineabrufe vgl. BVerfG, NJW 2007, 2464 (2470).

4.3. § 9 Abs. 4 BVerfSchG, § 5 BNDG, § 5 MADG

4.3.1. Genese der Regelungen

§ 9 Abs. 4 BVerfSchG erlaubt es dem BfV, den Standort eines aktiv eingeschalteten Mobilfunkendgeräts bzw. dessen Karten- oder Gerätenummer durch Simulation einer Mobilfunkzelle (kein Eingriff in Art. 10 GG) zu ermitteln. Eingeführt wurde die Vorschrift durch das TBG im Jahre 2002.[114] Die Maßnahme setzte voraus, dass gemäß § 3 Abs. 1 G 10 tatsächliche Anhaltspunkte für den Verdacht einer bestimmten Straftat vorlagen. Nach der Gesetzesbegründung sollte die Regelung v.a. dazu dienen, TKÜ-Maßnahmen nach dem G 10 vorzubereiten.[115] Das TBEG 2007 löste die Bestimmung vom strafrechtlichen Kontext und verwies auf die Voraussetzungen des § 8a Abs. 2 BVerfSchG.[116] Die Maßnahme diene auch zur Vorbereitung von Auskünften über Verbindungsdaten. Zudem sei der Verweis auf die Voraussetzungen nach dem G 10 nicht angemessen.[117] Bis zum Jahre 2007 war die Maßnahme nur zur Erfüllung der Aufgaben gemäß § 3 Abs. 1 Nr. 2-4 BVerfSchG möglich. Seit dem TBEG kann der IMSI-Catcher auch zum Schutz der freiheitlichen demokratischen Grundordnung eingesetzt werden, sofern die besonderen Voraussetzungen des § 8a Abs. 2 S. 2 BVerfSchG erfüllt sind. Die Erstreckung auf Bestrebungen gegen die freiheitliche demokratische Grundordnung erfolgte, „da auch in diesen Aufklärungsbereichen Verbindungen zwischen Zielpersonen und deren Aufenthalt von gleichem Aufklärungsinteresse sind.“[118] Durch das Änderungsgesetz 2011 wurde der Verweis auf die Einschränkung des Art. 10 Abs. 1 GG gestrichen.[119] Formell erfolgte eine Umstellung des S. 7 auf den neu gefassten § 8b Abs. 1-3 BVerfSchG (zuvor: § 8a Abs. 4-6 BVerfSchG). Das Verfahren gemäß § 8b Abs. 1 BVerfSchG wurde beibehalten trotz vereinzelter Kritik, dass dieses Antragsverfahren zu Verzögerungen führe.[120]
§ 5 MADG bestand bereits vor dem Jahre 2002. Seit dem TBG verweist § 5 Hs. 2 MADG auf § 9 Abs. 2-4 BVerfSchG statt wie zuvor nur auf § 9 Abs. 2-3 BVerfSchG.[121] Die Änderung erlaubt den Einsatz des IMSI-Catchers für das BAMAD. Der Gesetzgeber begründet die Einführung mit der gleichgelagerten Aufgabenstellung von BfV und BAMAD.[122]
§ 3 S. 2 BNDG sah eine entsprechende Anwendung der Maßnahmen nach § 9 BVerfSchG vor. Die Regelung wurde im Zuge der Reform des BNDG Ende 2016 in § 5 verschoben.[123]

4.3.2. Empirische Ergebnisse

Das Verfahren zur Beantragung einer Anordnung zum Einsatz des IMSI-Catchers läuft entsprechend der Beantragung von G 10-Maßnahmen ab. Das BMI entscheidet – auch bei Anordnungen für Maßnahmen des BND und BAMAD – darüber, ob ein Antrag gestellt und an die G 10-Kommission weitergeleitet wird. Die Zusammenarbeit mit BMI, BMVg bzw. BKAmt funktioniere aus Sicht der drei Nachrichtendienste bislang gut, da es sich aufgrund der Erfahrungen aus dem G 10-Bereich um ein eingespieltes Verfahren handele. Eine Besonderheit

---

[114] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 362, in Kraft getreten am 01.01.2002.
[115] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 40.
[116] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 3, in Kraft getreten am 11.01.2007.
[117] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 15 f.
[118] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 16.
[119] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2578, in Kraft getreten am 10.01.2012.
[120] Zur Kritik BMI, Bericht der Bundesregierung zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (nur Entwurf), 2011, S. 81.
[121] Art. 2 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 363, in Kraft getreten am 01.01.2002.
[122] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 42.
[123] Art. 1 Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23.12.2016, BGBl I Nr. 67 vom 30.12.2016, S. 3346.

hinsichtlich der Nutzung dieses Instruments ergibt sich beim BAMAD, der nicht – wie die beiden anderen Nachrichtendienste – über einen eigenen IMSI-Catcher verfügt, sondern zur Umsetzung der Maßnahme andere Bundes- oder Landesbehörden um Amtshilfe bittet.
Im Erhebungszeitraum wurde der IMSI-Catcher hauptsächlich vom BfV zur verdeckten Datenerhebung genutzt, das insgesamt 17 Anwendungsfälle übermittelte. Allerdings wurde die Maßnahme nur in 15 Fällen auch tatsächlich umgesetzt. In einem Fall wurde der Einsatz des IMSI-Catchers angeordnet, ohne dass es zur Umsetzung der Maßnahme kam. In einem weiteren Fall konnte die Maßnahme aufgrund von Kapazitätsengpässen nicht umgesetzt werden, sodass keine Daten erhoben wurden.
Das BAMAD machte im Erhebungszeitraum ein einziges Mal von der Möglichkeit Gebrauch, Daten mittels IMSI-Catcher zu erheben. In diesem konkreten Fall sei der IMSI-Catcher Bestandteil eines Maßnahmen-Bündels gewesen. Er sei zum Einsatz gekommen, da die betroffene Person beim Telefonieren beobachtet worden sei, im Rahmen einer parallel laufenden TKÜ jedoch keine Kommunikation festgestellt werden konnte. Dadurch habe ein weiterer Kommunikationsweg ermittelt werden können, der in die laufende G 10-Maßnahme einbezogen worden sei. Hingegen kam das Instrument beim BND im Erhebungszeitraum nicht zum Einsatz.
Dies deckt sich im Wesentlichen mit den Erfahrungen aus den vergangenen Jahren. So wurde der IMSI-Catcher im Jahr 2015 insgesamt 18 Mal angeordnet, wobei das BfV 17 Mal und das BAMAD ein einziges Mal auf die Maßnahme zurückgriffen.[124] Beim BND liege es daran, dass der IMSI-Catcher nur bei sehr schwerwiegenden Verdachtsfällen im Bereich Spionageabwehr zur Eigensicherung bzw. bei der Abwehr von Angriffen auf den BND in seiner Gesamtheit zum Einsatz gekommen sei. Hierbei handele es sich jedoch um Ausnahmefälle.

Gründe für die Anordnung des IMSI-Catchers

Die Maßnahmen wurden aus unterschiedlichen Gründen beantragt und angeordnet. Folgende Tabelle gibt einen Überblick, wie oft die jeweiligen Normen genannt wurden:

[124] Vgl. Deutscher Bundestag, BT-Drs. 18/11228, S. 10.

Tab. 8: Gründe für den Einsatz des IMSI-Catcher

Gründe der Datenerhebung	**Anzahl Nennungen** (Mehrfach-nennungen möglich)
Aufgrund von Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben (§ 3 Abs. 1 Nr. 1 BVerfSchG)	12
Aufgrund von Bestrebungen, die bezwecken oder auf Grund ihrer Wirkungsweise geeignet sind, zu Hass oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumden anzugreifen und dadurch die Bereitschaft zur Anwendung von Gewalt zu fördern und den öffentlichen Frieden zu stören oder (§ 3 Abs. 1 Nr. 1 i. V. m. § 8a Abs. 2 S. 2 Nr. 1 BVerfSchG)	*(-)*
Aufgrund von Bestrebungen, die bezwecken oder auf Grund ihrer Wirkungsweise geeignet sind, Gewalt anzuwenden oder vorzubereiten, einschließlich dem Befürworten, Hervorrufen oder Unterstützen von Gewaltanwendung, auch durch Unterstützen von Vereinigungen, die Anschläge gegen Personen oder Sachen veranlassen, befürworten oder androhen (§ 3 Abs. 1 Nr. 1 i. V. m. § 8a Abs. 2 S. 2 Nr. 2 BVerfSchG)	*(11)*
Aufgrund von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht (§ 3 Abs. 1 Nr. 2 BVerfSchG)	5
Aufgrund von Bestrebungen im Geltungsbereich dieses Gesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden (§ 3 Abs. 1 Nr. 4 BVerfSchG)	9
Aufgrund von Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 GG), insbesondere gegen das friedliche Zusammenleben der Völker (Art. 26 Abs. 1 GG) gerichtet sind (§ 3 Abs. 1 Nr. 4 BVerfSchG)	8
Aufgrund sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht (§ 1 Abs. 1 S. 1 Nr. 2 MADG)	1
Gesamtzahl	**35**

Am häufigsten wurde die Anordnung des IMSI-Catchers auf § 3 Abs. 1 Nr. 1 BVerfSchG (12) sowie auf § 3 Abs. 1 Nr. 3 BVerfSchG (9) gestützt. In knapp der Hälfte der Fälle begründete das BfV die Notwendigkeit des IMSI-Catcher-Einsatzes auch mit der durch das TBG neu eingeführten Aufgabennorm (§ 3 Abs. 1 Nr. 4 BVerfSchG) (8).
In neun Fällen stützte sich die Anordnung auf nur eine Aufgabennorm (je 4x auf § 3 Abs. 1 Nr. 1 BVerfSchG bzw. § 3 Abs. 1 Nr. 2 BVerfSchG und 1x auf § 1 Abs. 1 S.1 Nr. 2 MADG). In weiteren acht Fällen wurde Bezug auf drei Aufgabennormen genommen (8x § 3 Abs. 1 Nrn. 1, 3 und 4 BVerfSchG). In einem Fall wurde der Einsatz des IMSI-Catchers mit zwei Aufgabennormen (§ 3 Abs. 1 Nrn. 1 und 3 BVerfSchG) begründet.
Ein eindeutiger Schwerpunkt des IMSI-Catcher-Einsatzes zeigte sich beim Blick auf die einschlägigen Phänomenbereiche. In knapp der Hälfte der Fälle (8) wurde die Maßnahme im Zusammenhang mit *Islamismus* genutzt. In sechs Fällen ging es hingegen um *Proliferation und Spionage* und in vier Fällen um *Rechts-/Linksextremismus*. Im Bereich Ausländerextremismus wurde der IMSI-Catcher im Erhebungszeitraum nicht eingesetzt. Im Bereich Islamismus ging es im Wesentlichen um die Unterstützung islamistischer/terroristischer Vereinigungen (8). Im Bereich Proliferation und Spionage bestand der Verdacht einer geheimdienstlichen Tätigkeit im Geltungsbereich des BVerfSchG bzw. MADG (6). Dagegen kam die Maßnahme im Bereich Rechts-/Linksextremismus aufgrund der Unterstützung eines gewaltorientierten linksextremistischen Personenzusammenschlusses (3) und aufgrund der Planung, Vorbereitung und Durchführung von gegen linksorientierte Personen gerichtete Straftaten (1) zum Einsatz.

Betroffene Personen

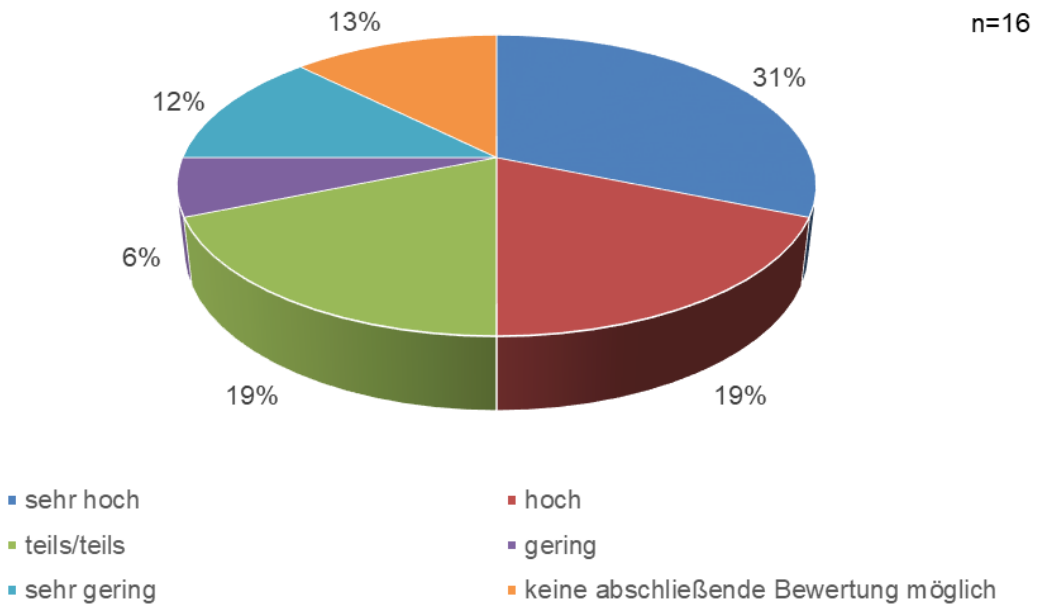
Im Erhebungszeitraum richteten sich die Anordnungen für den Einsatz des IMSI-Catchers gegen insgesamt 23 Hauptbetroffene, bei denen tatsächliche Anhaltspunkte dafür vorlagen, dass sie die schwerwiegenden Gefahren nach § 8a Abs. 2 und 2a BVerfSchG nachdrücklich fördern. In einem Fall richtete sich die Anordnung zusätzlich gegen eine Person, bei der aufgrund bestimmter Tatsachen anzunehmen ist, bei Auskünften nach Absatz 2 Satz 1 Nummer 4, dass sie für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Mitteilungen entgegennimmt oder weitergibt, oder dass eine Person nach Nummer 1 ihren Anschluss benutzt. Im Großteil der Fälle (14) richtete sich die Anordnung gegen eine Person. In vier Fällen betraf die Anordnung mehrere Personen (2x drei Hauptbetroffene, 1x zwei Hauptbetroffene sowie 1x ein Haupt- und ein Nebenbetroffener).
Dagegen wurden im Zuge der Maßnahme gemäß § 9 Abs. 4 BVerfSchG nur über 19 Personen (18 Hauptbetroffene und einen Nebenbetroffenen) auch tatsächlich Daten erhoben. In zwei Fällen erfolgte keine Datenerhebung, da die Maßnahme nicht umgesetzt wurde. BfV und BND betonten zudem, dass bei der Nutzung des IMSI-Catchers zwangsläufig auch Nummern Unbeteiligter erfasst würden, wobei diese jedoch im Gerät verblieben und nach der Ausfilterung der Nummer der Zielperson gelöscht würden.
In allen Fällen wurden im Zuge der Maßnahme sowohl die Geräte- als auch die Kartennummer und in zwei Fällen zusätzlich noch die Standortdaten zweier Hauptbetroffenen und eines Nebenbetroffenen ermittelt.
In 17 Fällen betrug der in der Anordnung festgelegte Zeitraum für die Nutzung des IMSI-Catchers drei Monate. In einem Fall wurden keine Angaben zum Zeitraum gemacht.
Im Anordnungszeitraum wurde der IMSI-Catcher in den meisten Fällen (10) nur einmal eingesetzt. In fünf Fällen wurde der IMSI-Catcher zweimal und in einem weiteren Fall fünfmal eingesetzt. In zwei Fällen erfolgte kein Einsatz des IMSI-Catchers. Im Durchschnitt dauerte ein IMSI-Catcher-Einsatz 4,1 Tage, wobei die Einsatzdauer zwischen einem Tag und sieben Tagen

variierte. In einem Fall wurden keine konkreten Angaben zur Dauer des Einsatzes des IMSI-Catchers gemacht.

Nutzen der gewonnenen Informationen

Wie hilfreich das Instrument für die nachrichtendienstliche Arbeit ist, zeigt sich anhand der mittels IMSI-Catcher gewonnenen Daten. In acht Fällen wurde der Nutzen als hoch bzw. sehr hoch eingeschätzt, während in drei Fällen der Nutzen der gewonnenen Informationen als gering bzw. sehr gering eingestuft wurde. In weiteren drei Fällen waren die gewonnenen Informationen teilweise von Nutzen für die nachrichtendienstliche Arbeit. In zwei Fällen war hingegen keine abschließende Bewertung möglich.

Abb. 5: Bewertung des Nutzens der mittels IMSI-Catcher gewonnenen Informationen durch das BfV und BAMAD



Folgende Begründungen wurden für die einzelnen Bewertungen genannt:

Tab. 9: Begründungen des BfV und BAMAD für die Nutzenbewertung der mittels IMSI-Catcher gewonnenen Informationen[125]

Bewertung und Begründung	Anzahl
Sehr hoher Nutzen	**5**
Die Daten flossen in eine laufende G 10-Maßnahme ein. In der Folge stieg das relevante Informationsaufkommen	1
Durch die IMSI-Maßnahme konnten mehrere Mobilfunkanschlüsse von Linksextremisten generiert werden, die nicht auf diese Personen registriert waren. Somit konnten im Anschluss TKÜ-Maßnahmen durchgeführt werden.	1
Es wurden IMSI eines erwarteten ausländischen Mobilfunknetzes festgestellt.	1
Durch die Maßnahme konnte ausgeschlossen werden, dass der Betroffene keine dem Fachbereich unbekannten Mobilfunknummern nutzt.	2
Hoher Nutzen	**3**
Die Hauptbetroffenen wechseln sehr häufig ihre Rufnummer, so dass eine lückenlose zielgerichtete Auswertung zur Erforschung des Anfangsverdachts der Unterstützung einer terroristischen Vereinigung im Ausland nur unter Einbeziehung des IMSI-Catchers erfolgen kann. Eine zweckmäßige Auswertung einer Beschränkungsmaßnahme bedarf der Überwachung aller durch die Hauptbetroffenen genutzten Rufnummern. Sofern sich die Hauptbetroffenen konspirativ verhalten, ist eine Erfassung all ihrer genutzten Rufnummern allein durch eine Beschränkungsmaßnahme nicht zu gewährleisten.	1
Es [wurde] vermutet, dass der Betroffene weitere Mobiltelefone nutzt. Es konnten ihm jedoch keine weiteren zugeordnet werden, die er alleine nutzt. Insofern wurde die bekannte Nummer bestätigt. Es konnten darüber hinaus durch die begleitende Observation festgestellt werden, dass der Betroffene das Mobiltelefon einer Kontaktperson mit nutzte.	1
Im durchgeführten Zeitraum konnte eine IMSI/IMEI-Nummer ermittelt werden.	1
Teilweise von Nutzen	**3**
Es wurden keine neuen IMSI/IMEIs festgestellt. Entweder die fraglichen Mobilfunkgeräte wurde zum Messzeitpunkt nicht genutzt oder der Ursprungshinweis hat sich als falsch herausgestellt.	2

[125] In Anbetracht unterschiedlicher Kontexte des Einsatzes des IMSI-Catchers können inhaltlich ähnliche Begründungen zu divergierenden Nutzenbewertungen führen.

Zwar konnten tatsächlich keine weiteren Mobilfunktelefone des Hauptbetroffenen festgestellt werden, jedoch konnte über die Gewissheit erlangt werden, dass die Person entgegen den ursprünglichen Beobachtungen hauptsächlich mit einem Gerät kommuniziert.	1
Geringer Nutzen	**1**
Durch die IMSI-Catcher-Maßnahme konnten keine weiteren IMSIs, die durch den Betroffenen genutzt wurden, festgestellt werden. Möglicherweise nutzt der Betroffene keine weiteren Rufnummern.	1
Sehr geringer Nutzen	**2**
Es konnte keine neue Rufnummer in Erfahrung gebracht werden.	1
Im Zeitraum der Maßnahme fanden zwei Einsätze statt. Die Messungen erbrachten keine konkreten Zuordnungen von IMSI/IMEI.	1
Keine abschließende Bewertung möglich	**2**
Es konnten keine weiteren Daten gewonnen werden.	1
Trotz mehrfacher Messungen an verschiedenen Standorten war es nicht möglich, eine weitere Nummer des Hauptbetroffenen zu erheben. Dieses ist aber nach hiesiger Einschätzung nicht in einem Messfehler begründet, sondern in der schlichten Tatsache, dass der Hauptbetroffene kein weiteres (unbekanntes) Endgerät benutzte.	1

Im Anhang sind zudem einige Fallbeispiele aufgeführt, die darlegen, welcher konkrete Nutzen mit dem Einsatz des IMSI-Catchers verbunden war (siehe Anhang, S. 158). Das BfV und das BAMAD wiesen zudem darauf hin, dass es im Erhebungszeitraum keine technischen Probleme beim Einsatz des IMSI-Catchers gab.

Mitteilungs- und Löschungspflicht

In keinem Fall erfolgte eine Unterrichtung der Betroffenen, über die im Zuge der Maßnahmen Daten erhoben wurden. Begründet wurde dies in erster Linie damit, dass aufgrund der erst kürzlich erfolgten Beendigung eine Entscheidung über die Unterrichtung des/der Betroffenen noch ausstehe. In vier Fällen wurde darauf hingewiesen, dass die Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden konnte. In zwei Fällen erfolgte keine Umsetzung der Maßnahme und somit auch keine Datenerhebung. In einem Fall gab das BfV an, dass es weitere Maßnahmen gegen den Betroffenen geben würde, die durch eine Unterrichtung gefährdet würden.

Mitteilungsverfahren gemäß § 8b Abs. 7 BVerfSchG (2015-2017)

Da zu den Maßnahmen, die zwischen dem 1. Oktober 2016 und dem 30. September 2017 abgeschlossen und übermittelt wurden, noch keine Entscheidung vorlag, ob die Betroffenen hierüber unterrichtet werden können oder nicht, wurden die drei Nachrichtendienste darum gebeten, Informationen zu Mitteilungsprüfungen für den Zeitraum 1. Januar 2015 bis 31. Dezember 2017[126] zur Verfügung zu stellen. Hierbei handelte es sich um evaluierungs-

[126] Das BfV konnte aus organisatorischen Gründen nur Informationen für den Zeitraum 1. Januar 2015 bis 30. Juni 2017 zur Verfügung stellen.

pflichtige Maßnahmen gemäß § 9 Abs. 4 BVerfSchG, die nicht im Erhebungszeitraum abgeschlossen worden waren. Diese zusätzlichen Informationen sollten dazu dienen, einen besseren Eindruck zu bekommen, wie sich die Mitteilungspraxis bei den drei Nachrichtendiensten darstellt.

BfV

Die Prüfung, ob den Betroffenen mitzuteilen sei, dass gegen sie eine Anordnung gemäß § 9 Abs. 4 BVerfSchG gerichtet war, erfolgte bei BfV, BND und BAMAD nach dem gleichen Schema wie bei den besonderen Auskunftsverlangen. Die Mitteilungsüberprüfungen des BfV verliefen bei 21 Maßnahmen nach § 9 Abs. 4 BVerfSchG zu 27 Hauptbetroffenen positiv. Dagegen wurde bei 52 Maßnahmen die Mitteilung an 59 Betroffene (57 Haupt- und zwei Nebenbetroffene) zurückgestellt, da bei einer Mitteilung eine Gefährdung des Zwecks der Beschränkungsmaßnahme und/oder der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes nicht ausgeschlossen werden konnten. Die G 10-Kommission gab in allen Fällen dem Antrag auf Zurückstellung, die in der Regel für zwei Jahre, teilweise aber auch für einen kürzeren Zeitraum erfolgte, statt. Zudem stimmte die G 10-Kommission bei Maßnahmen zu vier Hauptbetroffenen einer endgültigen Nichtmitteilung zu. Nach Aussage des BfV könne es Fälle geben, in denen der Betroffene aus praktischen Gründen nicht unterrichtet werde, etwa wenn die Betroffenen Aliasnamen bzw. Fiktivpersonalien verwenden würden, die wahre Identität nicht bekannt sei, die Betroffenen verstorbenen seien oder eine Anschrift nicht mehr ermittelt werden könne.[127] Eine Statistik hierzu wird seit dem 1. Halbjahr 2017 im BfV geführt. Für den Erhebungszeitraum konnte daher auch nur diesbezüglich eine Aussage getroffen werden. Eine Nichtzustellung aus praktischen/faktischen Gründen gab es in diesem Zeitraum nicht.
Im abgefragten Zeitraum gab es weder Beschwerden noch Klageverfahren. Teilweise wendeten sich die Betroffenen telefonisch an das BfV, um weitere Erläuterungen zu der Beschränkungsmaßnahme zu erhalten.

BAMAD

Das BAMAD traf im Zusammenhang mit einem IMSI-Catcher-Einsatz aus dem Jahr 2015 die Entscheidung, einem Hauptbetroffenen die Maßnahme mitzuteilen. In demselben Fall, bei dem die Maßnahme gegen zwei weitere Hauptbetroffene angeordnet, jedoch nicht umgesetzt wurde, wurde nach Prüfung im September 2017 entschieden, dass keine weitere Mitteilungsprüfung mehr erfolgt. Zwischen 2015 und 2017 gab es einen Antrag auf Zurückstellung der Mitteilung für zwei Jahre. Begründet wurde die Zurückstellung damit, dass mit der Mitteilung ein absehbarer Eintritt übergreifender Nachteil für das Wohl des Bundes verbunden wäre. Im Erhebungszeitraum wurde kein Antrag auf Zurückstellung des BAMAD von der G 10-Kommission abgelehnt. Zudem wurden von den Betroffenen in keinem Fall Rechtsmittel eingelegt.

BND

Beim BND gab es im Zeitraum 1. Januar 2015 bis 31. Dezember 2017 keinen Fall, in dem einem Betroffenen mitgeteilt wurde, dass Daten gemäß § 5 BNDG i. V. m. § 9 Abs. 4 BVerfSchG über ihn erhoben wurden. Bei den beiden Fällen aus dem vierten Quartal 2017 konnte es noch zu keiner Mitteilung an die Betroffenen kommen, da die entsprechenden Mitteilungsentscheidungen bis zum 31. Dezember 2017 noch nicht getroffen worden waren.

[127] So die Auskunft des BfV.

Bewertung und Optimierungsbedarf aus Sicht der Nachrichtendienste

Alle drei Nachrichtendienste waren der Auffassung, dass es sich beim IMSI-Catcher um ein sinnvolles und nützliches Instrument der Informationserhebung handle, mit dem gezielt Nummern erfasst werden könnten, um damit (zusätzliche) G 10-Maßnahmen vorzubereiten. Dies gelte insbesondere für Personen, die damit rechnen, überwacht zu werden und deshalb z. B. regelmäßig die SIM-Karte wechseln (sog. Kartenspieler). Ein weiterer Vorteil aus Sicht des BAMAD sei, dass dies die einzige Möglichkeit darstelle, ausländische Rufnummern zu erfassen.
Von allen drei Nachrichtendiensten wurde moniert, dass das Beantragungsverfahren vor allem unter Berücksichtigung der geringen Eingriffstiefe des IMSI-Catchers, des teilweise hohen Zeitdrucks und der begrenzten Ressourcen sehr aufwendig sei. In diesem Zusammenhang wurde auch durch das BfV auf die sehr hohe Eingriffsschwelle hingewiesen, obwohl es sich hierbei nicht um einen Eingriff in Art. 10 GG handeln würde. Insgesamt solle das Verfahren praktikabler gestaltet werden. Das BfV plädierte hier für ein hausinternes Genehmigungsverfahren ohne Beteiligung des BMI und der G 10-Kommission. Somit entfiele sowohl das Anordnungsverfahren als auch die Mitteilungspflicht.
Der BND regte beispielsweise an, das Verfahren auf die Ebene der Datenverwendung anstatt auf Ebene der Datenerhebung anzusiedeln. Es sollte nur dann zur Anwendung gebracht werden, wenn die Maßnahme erfolgreich gewesen sei, d. h. eine Nummer ermittelt wurde. Diese dürfte in der Folge nur verwendet werden, wenn dies förmlich (derzeit etwa durch die G 10-Kommission) genehmigt würde.
Zudem wies das BAMAD darauf hin, dass die Möglichkeit häufiger genutzt würde, wenn es über einen eigenen IMSI-Catcher verfügen würde. Derzeit sei man immer auf die Amtshilfe von anderen Sicherheitsbehörden angewiesen. Aufgrund der limitierten Anzahl von Geräten sei es in der Vergangenheit schon vorgekommen, dass das BAMAD Maßnahmen nicht hätte durchführen können. Zudem regte das BAMAD an, die Befugnis zur Anordnung des IMSI-Catchers auf das BMVg zu übertragen, da dadurch eine sinnvolle Bündelung der Anordnungsbefugnisse beim BMVg erreicht werden könnte.

4.3.3. Rechtswissenschaftliche Bewertung

Für die verfassungsrechtliche Bewertung der empirisch erhobenen Anwendungspraxis ist zunächst darauf hinzuweisen, dass das BVerfG den Einsatz eines IMSI-Catchers auf der Grundlage von § 100i StPO nicht beanstandet hat.[128] Die Grundsätze der Entscheidung lassen sich auch auf die vorliegend relevanten Bestimmungen übertragen.
Nach Auffassung des BVerfG stellt der Einsatz eines IMSI-Catchers keinen Eingriff in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG dar, da ausschließlich technische Geräte miteinander kommunizieren.[129] Der Betroffene und unbeteiligte Dritte werden in ihrem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG beeinträchtigt. Soweit in der Zeit des Einsatzes ein Rufaufbau verhindert wird, liegt ein Eingriff in die allgemeine Handlungsfreiheit gemäß Art. 2 Abs. 1 GG vor.

[128] Vgl. BVerfG, Beschl. v. 22. 8. 2006 – 2 BvR 1345/03 –, NJW 2007, S. 351 ff.
[129] BVerfG, Beschl. v. 22. 8. 2006 – 2 BvR 1345/03 –, NJW 2007, S. 351 (353); Ebenso Mallmann, in: Schenke/Graulich/Ruthig, Sicherheitsrecht, 2014, § 9 BVerfSchG Rn. 38; Bundesregierung, BT-Drs. 17/6925, S. 17.

Die Maßnahme dient dem Schutz hochrangiger verfassungsrechtlicher Güter, wie sie in § 3 Abs. 1 BVerfSchG normiert sind, und damit der Effektuierung der nachrichtendienstlichen Tätigkeit in der modernen Mediengesellschaft.[130]
Die aus der empirischen Erhebung ermittelte Anwendungspraxis enthält keine Anhaltspunkte, dass der Einsatz des IMSI-Catchers ungeeignet zur Erreichung des Schutzes dieser Güter war. Vielmehr sind in der überwiegenden Zahl der Fälle Daten erhoben worden, die für die Arbeit des BfV von hoher oder sehr hoher Relevanz waren.
Die Erforderlichkeit der Maßnahmen ergibt sich im Regelfall bereits aus dem Vorliegen der Tatbestandsvoraussetzungen des § 9 Abs. 4 S. 2 BVerfSchG, wonach ohne den Einsatz des IMSI-Catchers die Ermittlung des Standortes oder die Ermittlung der Geräte- oder Kartennummer aussichtslos oder wesentlich erschwert sein muss. Im Einzelfall gleichwohl zu Gebote stehende mildere Mittel, wie die Einholung von Auskünften bei Telekommunikationsdienstleistern nach §§ 112, 113 TKG[131], sind genutzt worden und haben im Erfolgsfalle dazu geführt, dass der Einsatz des IMSI-Catchers unterblieben ist. Umgekehrt stellt sich die Anfrage bei Telekommunikationsdienstleistern angesichts der besonderen Organisationsform und Anpassung der Strukturen der Beobachtungsobjekte regelmäßig als nicht gleich geeignet dar.
Hinweise darauf, dass die sich aus der gebotenen Verhältnismäßigkeit im engeren Sinne ergebenden Anforderungen durch Maßnahmen nach § 9 Abs. 4 BVerfSchG verfehlt worden sind, sind nicht erkennbar. Die Maßnahmen dienen dem Schutz hochrangiger Rechtsgüter und sind von den Nachrichtendiensten angesichts von 18 Anordnungen über den Erhebungszeitraum von 12 Monaten äußerst zurückhaltend eingesetzt worden. Anordnungen nach § 9 Abs. 4 BVerfSchG sind offenbar auf das zur Zweckerreichung unabdingbare Maß beschränkt worden. In aller Regel beschränkte sich die Maßnahme auf eine Person, nur in zwei Fällen wurden auch die Standortdaten erfasst und nur in einem Fall wurde eine Verlängerung der Maßnahme beantragt.
Dass die bei Maßnahmen nach § 9 Abs. 4 BVerfSchG zwangsläufig erfassten Nummern Unbeteiligter im Gerät verbleiben und nach Ausfilterung der Nummer der Zielperson gelöscht werden, entspricht den vom BVerfG formulierten Anforderungen[132].
Eine rechtliche Bewertung des Umgangs mit der Pflicht zur Benachrichtigung Betroffener nach § 9 Abs. 4 S. 6, § 8b Abs. 7 S. 1 BVerfSchG, § 12 Abs. 1 G 10 lässt keine Verfassungsrecht verletzende Handhabung erkennen. Die Mitteilung wird für jeden Einzelfall geprüft, wobei eine eher recht häufige Zurückstellung dem Wesen des IMSI-Catchers als Vorfeldmaßnahme geschuldet ist, wodurch der Ermittlungserfolg – gerade auch der Anschlussmaßnahmen – typischerweise länger gefährdet werden kann.

[130] Vgl. Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011, S. 99.
[131] Vgl. Harnisch/Pohlmann, Der Einsatz des IMSI-Catchers zur Terrorismusbekämpfung durch das Bundeskriminalamt, NVwZ 2009, S. 1328 (1332) m.w.N.
[132] Siehe BVerfG, NJW 2007, S. 351 (356).

4.4. § 12 Abs. 3 BVerfSchG, § 20 Abs. 1 BNDG, § 6 Abs. 2 MADG

4.4.1. Genese der Regelungen

Nach § 12 Abs. 3 S. 2 BVerfSchG sind gespeicherte personenbezogene Daten über Bestrebungen gemäß § 3 Abs. 1 Nr. 1, 3 und 4 BVerfSchG spätestens zehn Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, der Behördenleiter oder sein Vertreter trifft im Einzelfall ausnahmsweise eine andere Entscheidung.
Bis zum Jahre 2002 lag die Frist für die Löschung von Maßnahmen nach § 3 Abs. 1 Nr. 1, 3 BVerfSchG bei zehn Jahren. Das TBG änderte die Differenzierung. Für Maßnahmen zum Schutz der freiheitlichen demokratischen Grundordnung galt eine Löschungsfrist von zehn Jahren, für die Maßnahmen nach § 3 Abs. 1 Nr. 3, 4 BVerfSchG eine Frist von 15 Jahren.[133] Der Gesetzgeber nahm an, dass sich Terroristen teilweise bewusst so konspirativ verhalten, dass neue Erkenntnisse erst nach zehn Jahren anfielen.[134] Der Gesetzgeber reduzierte im Jahre 2011 die Frist für Maßnahmen nach § 3 Abs. 1 Nr. 3, 4 BVerfSchG wieder auf zehn Jahre.[135] Die Frist von 15 Jahren habe sich als nicht erforderlich erwiesen, da die Norm nur wenige Fälle betroffen habe.[136]
Auf Maßnahmen nach § 3 Abs. 1 Nr. 2 BVerfSchG gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht findet § 12 Abs. 3 S. 2 BVerfSchG keine Anwendung. Eine maximale Löschungsfrist ist insoweit nicht vorgesehen, vielmehr erfolgt diese im Einzelfall und nach einer regelmäßigen, fünfjährigen Überprüfung nach § 12 Abs. 3 S. 1 BVerfSchG.
§ 6 Abs. 2 MADG hat folgenden Wortlaut: „Der Militärische Abschirmdienst hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, zu löschen und zu sperren nach § 12 des Bundesverfassungsschutzgesetzes.“ Die Bestimmung geht auf § 7 Abs. 1 der ursprünglichen Fassung des MADG aus dem Jahre 1990 zurück, die mit dem Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 inhaltlich unverändert als § 6 Abs. 2 MADG neugefasst wurde.
§ 5 Abs. 1 BNDG wurde im Jahre 1990 mit Erlass des BNDG eingefügt. Eine Änderung erfolgte durch das TBEG 2007.[137] Die Prüffrist des § 12 Abs. 3 S. 1 BVerfSchG für die Berichtigung und Löschung beträgt zehn Jahre, statt wie im BVerfSchG vorgesehen fünf Jahre. Zu der Verlängerung der Prüffrist führt die Gesetzesbegründung aus: „Der alleinige Verweis auf das Bundesverfassungsschutzgesetz hat sich bei den Prüffristen wegen der unterschiedlichen Aufgaben und Aufklärungsziele von BND und BfV nicht bewährt. Die Verweisung wird nun durch eine eigenständige Regelung zur Dauer der Prüffrist ergänzt, die auf die auftragsbedingten Besonderheiten der Datenverarbeitung beim BND Rücksicht nimmt.“[138] Mit der Novellierung Ende 2016 wurde die Regelung in § 20 Abs. 1 BNDG verschoben.

4.4.2. Empirische Ergebnisse

Durch das Gesetz zur Änderung des BVerfSchG wurden die bisher unterschiedlich geregelten Speicherfristen für das BfV vereinheitlicht. Während für die gemäß § 3 Abs. 1 Nr. 3 und 4 BVerfSchG erhobenen Daten vor der gesetzlichen Änderung eine Höchstspeicherfrist von 15

[133] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 363, in Kraft getreten am 01.01.2002.
[134] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 41; dafür auch Droste, Handbuch (2007), S. 433.
[135] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2578, in Kraft getreten am 10.01.2012.
[136] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 17.
[137] Art. 3 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 5, in Kraft getreten am 11.01.2007.
[138] Bundesregierung, BT-Drs. 16/2921, S. 19.

Jahren galt, wurde diese durch das Änderungsgesetz auf zehn Jahre herabgesetzt. Lediglich für Informationen, die im Zusammenhang mit § 3 Abs. 1 Nr. 2 BVerfSchG gespeichert wurden, existiert eine solche maximale Speicherungsfrist nicht. Entsprechend gilt die Verkürzung der Speicherfrist für das BAMAD nach § 1 Abs. 2 S. 2 MADG. Für den BND hat sich hingegen nichts geändert, da er bereits vor dem Änderungsgesetz der Höchstspeicherfrist nicht unterworfen war.[139] Durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes aus dem Jahr 2015 wurde zudem eine verfahrensrechtliche Änderung vorgenommen. Anstelle des Präsidenten des BfV/BAMAD bzw. seines Vertreters entscheidet nun die Abteilungsleitung bzw. seine Stellvertretung darüber, ob von einer Löschung personenbezogener Daten nach 10 Jahren abgesehen wird.

Im Erhebungszeitraum gab es weder beim BfV noch beim BAMAD einen Fall, in dem aufgrund der Entscheidung der Abteilungsleitung bzw. seiner Stellvertretung personenbezogene Daten gemäß § 12 Abs. 3 S. 2 BVerfSchG bzw. § 6 Abs. 2 MADG nach 10 Jahren *nicht* gelöscht wurden. Grundsätzlich würden aus dem beim BfV betriebenen NADIS WN darin gespeicherte Personen nach § 12 Abs. 3 Satz 2 BVerfSchG automatisch unter Protokollierung des Löschungsvorgangs gelöscht, wenn nicht nach einer entsprechenden Prüfung Gründe festgestellt werden, die eine weitere Speicherung rechtfertigen. Die Gründe für die Löschungen würden dabei allerdings nicht protokolliert. Lägen hingegen Gründe vor, die eine Weiterspeicherung rechtfertigen, würden entsprechende Eingaben, die ihrerseits vollständig protokolliert werden, erfolgen.

Beim BfV orientiert sich die Dauer der Speicherung am sog. „Erkenntnisdatum“. Das Erkenntnisdatum bezeichnet das Datum „der letzten relevanten Erkenntnis“. Dieses kann nur dann hochgesetzt werden, wenn Erkenntnisse vorliegen, die eine Neuspeicherung der Daten rechtfertigen würden. Als Beispiel ist hier die erneute Aufnahme einer Zielperson in den Leitungsbereich einer terroristischen Organisation zu nennen, während z. B. die Aktualisierung einer Adresse nicht ausreichend ist. Ein halbes Jahr vor Ablauf der Zehnjahresfrist würden die jeweiligen Daten dem Sachbearbeiter elektronisch vorgelegt. Komme der Sachbearbeiter bei seiner Prüfung zu dem Schluss, dass die Daten weiterhin relevant seien, müsse die Beibehaltung der Daten von der Abteilungsleitung genehmigt werden. Eine Besonderheit bei der Datenlöschung ergebe sich derzeit aus den NSU- und NSA-Moratorien, da diese Daten nicht gelöscht, sondern in eine Quarantäne verschoben worden seien. Das BfV wies zudem daraufhin, dass die Verlängerungsprüfung gemäß § 12 Abs. 3 S. 2 BVerfSchG aufgrund der Vielzahl der Fälle sehr aufwendig sei, jedoch nur in Einzelfällen von einer Löschung der Daten abgesehen werde.

Das BAMAD gab an, dass die Relevanz einer Information danach bewertet werde, ob diese Informationen noch Erkenntnisse für die Aufgabenerledigung oder ein anhängiges Gerichtsverfahren benötigt würden. Mit Hilfe des Dokumentenmanagementsystems werde alle fünf Jahre geprüft, ob die gespeicherten Informationen noch benötigt würden. Falls die Daten nicht mehr relevant sind, würden diese dann gelöscht. Allerdings seien im Erhebungszeitraum aufgrund des NSU-Aktenvernichtungsmoratoriums keine Daten gelöscht, sondern auf ein „Sperr“-Konto verschoben worden, zu dem nur die zuständigen Datenschutzbeauftragten sowie der Beauftragte des BMVg für den NSU-Untersuchungsausschuss und die ihm zugewiesenen Beschäftigten des BAMAD Zugang haben.

Der BND verwies in diesem Zusammenhang darauf, dass er für die Rechtfertigung einer Speicherfristverlängerung die nachrichtendienstliche Relevanz der gespeicherten personenbezogenen Daten heranziehe. Personenbezogene Daten würden zudem bei der Speicherung als solche markiert. Dabei werde die Speicherdauer festgelegt und die Datensätze mit einer

[139] Vgl. dazu sogleich bei der Bewertung durch den BND.

Löschwiedervorlage versehen. Die Überprüfung der gespeicherten personenbezogenen Daten erfolge mit anstehendem Ablauf der so festgelegten Speicherfrist nach spätestens zehn Jahren. Über die Verlängerung der Speicherdauer oder Löschung der Daten entscheide der Auswerter. Bei Speicherung eines neuen Datums werde im Übrigen der gesamte Datensatz geprüft. Nach Auffassung des BND gelte die Höchstspeicherfrist im BVerfSchG nicht für den Auslandsnachrichtendienst, da zum einen das BNDG eine regelmäßige Überprüfung nach zehn Jahren vorsehe und es widersprüchlich sei, zugleich eine Höchstspeicherfrist von ebenfalls zehn Jahren vorzusehen. Zum anderen würde eine solche Höchstspeicherfrist im Widerspruch dazu stehen, dass es Aufgabe des BND sei, strategische Aufklärung zu betreiben. So würden in vielen Staaten bestimmte Eliten in wiederkehrenden Zyklen an die Macht kommen, die teils deutlich länger als zehn Jahren wären. Darüber hinaus würden aktuelle Vorgänge im Ausland nur unter Einbeziehung von erheblich länger als zehn Jahre zurückliegenden Ereignissen oder weiter als zehn Jahre zurückreichenden biographischen Details relevanter Akteure verständlich. Ohne eine entsprechend lange Speicherung dieser Daten, würden ggf. nachrichtendienstlich hochrelevante Informationen verloren gehen (so etwa über Mitglieder der Ba'ath-Partei im Irak, die mittlerweile teils Eliten des IS seien, oder Mitglieder der „Union of Islamic Courts" in Somalia, die nunmehr Führungspositionen bei al-Shabab innehaben). Somit stelle eine solche Datenspeicherung im BND eine Art institutionelles Gedächtnis dar.
Das BfV plädierte mit Verweis auf die NSU-Mordserie grundsätzlich für eine Verlängerung der Speicherfrist von zehn auf 15 Jahre. Hier habe es jahrelang keine neuen Erkenntnisse gegeben, da die entsprechenden Morde nicht zugeordnet werden konnten. Wenn nach zwölf oder 13 Jahren der Zusammenhang erkennbar werde, seien die relevanten Daten bereits gelöscht worden. Ein weiterer typischer Fall sind nach Angaben des BfV Funktionäre und „Parteisoldaten" terroristischer Parteien, die europa- oder weltweit rotieren und erst nach zehn Jahren wieder nach Deutschland zurückkehren würden. Diese Rückkehrer könnten dann u. U. nicht mehr zugeordnet werden, da auch hier die Daten bereits gelöscht worden seien.
Insgesamt gebe es vier Personengruppen, für die aus Sicht des BfV eine lange Speicherfrist wichtig wäre:

1. Konspirative Personen oder Vereinigungen, die schwer zu überwachen sind,
2. Personen in Haft,
3. Personen im Untergrund/Ausland,
4. Prägende Personen (z. B. RAF, Wehrsportgruppe Hoffmann).

In solchen Fällen sei es oft reiner Zufall, ob „zur richtigen Zeit" noch neue Erkenntnisse gewonnen werden könnten, die die Löschung der Daten aufschieben würden.
Auch das BAMAD sprach sich für deutlich längere Höchstspeicherfrist für personenbezogene Daten aus, da aufgrund der veränderten Karriereverläufe in der Bundeswehr, die dadurch gekennzeichnet seien, dass Personen aus dem Dienst ausscheiden und sich viele Jahre später wieder im Geschäftsbereich bewerben würden. Würde die Höchstspeicherfrist 15 oder 20 Jahre betragen, würden dem BAMAD auch Informationen zu Personen vorliegen, die mit 20 Jahren als Bundeswehrangehörige als Extremisten eigestuft wurden, daraufhin aus dem Dienst entlassen worden sind und sich mit Anfang/Mitte 30 wieder bei der Bundeswehr bewerben würden. Bei diesen Personen könne eine Einstellung nicht ausgeschlossen werden, da die entsprechenden Akten mittlerweile vernichtet worden wären. Zudem gelte im Bereich der Spionageabwehr auch heute schon eine Höchstspeicherfrist von 15 Jahren. Positiv bewertete das BAMAD die gesetzliche Änderung, dass anstelle des Präsidenten nun die Abteilungs-

leitung darüber entscheide, ob personenbezogene Daten nach Erreichung der Höchstspeicherfrist nicht gelöscht werden. Dies habe den Vorteil, dass die Abteilungsleitung einerseits näher am jeweiligen Fall „dran“ sei und andererseits solche Fälle nun schneller entschieden werden können.

4.4.3. Rechtswissenschaftliche Bewertung

Ausgehend von der in der Evaluierung zu unterstellenden Verfassungsmäßigkeit der § 12 Abs. 3 BVerfSchG, § 6 Abs. 2 MADG, § 20 Abs. 1 BNDG wirft die empirisch erhobene Anwendungspraxis keinen verfassungsrechtlichen Erörterungsbedarf mit Blick auf das Grundrecht auf informationelle Selbstbestimmung auf. Das Abstellen auf das sog. „Erkenntnisdatum“ zur Ermittlung des Beginns der Löschungsfrist führt zu einer die Grundrechte der Betroffenen weitestmöglich schonenden Auslegung des § 12 Abs. 3 S. 2 BVerfSchG. Auch das Informationsmanagement der automatisierten Vorlage zur Prüfung ist Ausdruck eines sensiblen Umgangs mit den personenbezogenen Daten. Dass von der ausnahmsweise bestehenden Möglichkeit der Nichtlöschung nach spätestens zehn Jahren Gebrauch gemacht wird, wenn die Daten noch zum Schutz der jeweiligen Rechtsgüter relevant sind, entspricht der gebotenen Abwägung zwischen dem Interesse am Schutz dieser Güter und den Grundrechten der Betroffenen, zumal es sich hierbei offenbar um absolute Ausnahmefälle handelt.

4.5. § 17 Abs. 3 BVerfSchG

4.5.1. Genese der Regelung

Europarechtlicher Hintergrund der Vorschrift ist das „Übereinkommen zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen (Schengener Übereinkommen) vom 14. Juni 1985“ und das „Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen vom 19. Juni 1990 (Schengener Durchführungsübereinkommen)“. Aufgrund des Beschlusses 2007/533/JI des Rates vom 12. Juni 2007 sollte das bisherige System durch eine zweite Generation ersetzt werden.[140] Mit nationalem Gesetz vom 6. Juni 2009 erfolgte die Aufhebung des Schengener Durchführungsübereinkommens (im Folgenden: SDÜ) und die Einführung des Schengener Informationssystems der zweiten Generation (SIS-II-Gesetz).[141] Art. 1 des SIS-II-Gesetzes erklärt die Bestimmung des Beschlusses 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) für anwendbar.
§ 17 Abs. 3 BVerfSchG wurde durch das TBEG im Jahre 2007 neu eingeführt.[142] Die Vorschrift verwies auf die damals geltende Bestimmung des Art. 99 Abs. 1, 3 und 4 SDÜ. Mit dem SIS-II-Gesetz vom 6. Juni 2009 erfolgte eine europarechtliche Anpassung. Verwiesen wird seitdem

[140] Vgl. Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), (ABl. L 205/2007, S. 63). Die Entwicklung des SIS II begann mit der Verordnung 2424/2001/EG (ABl. L 328/2001, S. 4 ff.) und dem Ratsbeschluss 2001/886/JI (ABl. L 328/2001, S. 1 ff.).
[141] Vgl. Art. 3 des Gesetzes zum Schengener Informationssystem der zweiten Generation (SIS II-Gesetz), BGBl I Nr. 30 vom 17. Juni 2009, in Kraft getreten am 09.04.2013.
[142] Art. 1 TBEG vom 05. Januar 2007, BGBl I Nr. 1 vom 10. Januar 2007, S. 3, in Kraft getreten am 11. Januar 2007.

auf Art. 36 und 37 des Beschlusses 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (im Folgenden kurz SIS II genannt).[143] Das SIS II ist seit dem 9. April 2013 in Betrieb.[144]
Die Neuregelung stellt eine Erleichterung dar: Das SIS II ermöglicht den Zugriff auf die ausgeschriebenen Daten durch alle Schengen-Vertragsstaaten, insbesondere anlässlich von Grenzkontrollen, in Echtzeit.[145] Im Jahr 2015 erfolgte eine redaktionelle Anpassung in Satz 6, der nunmehr auf § 8b Abs. 3 BVerfSchG verweist.[146]

4.5.2. Empirische Ergebnisse

Durch das TBEG ist für alle drei Nachrichtendienste die Möglichkeit geschaffen worden, Personen bzw. Sachen im Schengener Informationssystem II (SIS II) auszuschreiben. Wird eine ausgeschriebene Person bzw. Sache im Schengen-Raum kontrolliert, erhält die ausschreibende Behörde Informationen über mögliche Reisebewegungen sowie ggf. Mitreisende. Die Ausschreibung erfolgt unter bestimmten tatbestandlichen Voraussetzungen und wird von den Nachrichtendiensten per E-Mail an das BKA weitergeleitet, das für die Prüfung und Einstellung der Ausschreibung in das Fahndungssystem als nationale Sirene zuständig ist.

Anzahl der SIS II-Ausschreibungen

Im Erhebungszeitraum wurde die Möglichkeit von allen drei Nachrichtendiensten genutzt, wenn auch in unterschiedlichem Umfang. Am häufigsten griff der BND auf dieses Instrument zurück. Das BfV nutzte diese Möglichkeit ebenfalls regelmäßig, während des BAMAD lediglich zwei Ausschreibungen im Erhebungszeitraum vornahm. Dies liegt u. a. daran, dass sich der Zuständigkeitsbereich – anders als z. B. beim BfV – auf einen beschränkten Personenkreis (Angehörige des Geschäftsbereichs des BMVg) erstreckt, für den das Verlassen des Landes ohne Erlaubnis erhebliche Konsequenzen bedeuten kann. Im Vergleich zur vorherigen Evaluation ist festzustellen, dass die Zahl der SIS II-Ausschreibungen deutlich zugenommen hat. Das BfV und der BND begründeten die verstärkte Nutzung des Instruments mit der veränderten sicherheitspolitischen Lage (z. B. durch die Zunahme der Flüchtlingszahlen im Zuge des Syrienkonflikts). In diesem Zusammenhang wurde vom BND noch darauf hingewiesen, dass die Zunahme an Grenzübertritten relevanter Personen zugenommen habe, da Deutschland ein potenzieller Aktions- und Rückzugsort für Jihadisten v. a. aus Syrien und Irak geworden sei.

---

[143] Siehe Beschluss des Rates 2007/533/JI vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. Nr. L 205 S. 63 ff. Zur nationalen Umsetzung siehe Art. 3 des Gesetzes zum Schengener Informationssystem der zweiten Generation (SIS II-Gesetz), BGBl I Nr. 30 vom 17. Juni 2009, in Kraft getreten am 09.04.2013.
[144] Pressemitteilung der EU-Kommission: http://europa.eu/rapid/press-release_IP-13-309_de.htm
[145] Vgl. Tuffner, Bundeskriminalamt (1998), S. 239 (241).
[146] Art. 1 Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17.11.2015, BGBl I Nr. 45 vom 20.11.2015, S. 1941.

Tab. 10: Anzahl der SIS-Ausschreibungen (1.10.2016-30.9.2017)

Nutzer SIS II	Anzahl
BfV	314
BND	502
BAMAD	2
Gesamt	**818**

Gründe für die SIS II-Ausschreibungen

In 526 Fällen erfolgte eine Ausschreibung im SIS II zur Abwehr einer vom Betroffenen ausgehenden Gefährdung durch die drei Nachrichtendienste. In 183 Fällen gab es konkrete Anhaltspunkte für andere erhebliche Gefahren für die innere oder äußere Sicherheit. In zehn Fällen lagen der SIS II-Ausschreibung beide Anhaltspunkte zugrunde. In einem Fall wurden hierzu keine Angaben gemacht. Der BND nutzte das Instrument fast ausschließlich, das BAMAD ausschließlich, um Informationen zu gewinnen, die zur Abwehr anderer erheblicher Gefahren für die innere oder äußere Sicherheit erforderlich waren.

Tab. 11: Gründe für die Ausschreibung im SIS II

Anhaltspunkte für die Ausschreibungen	BfV	BND	BAMAD	Gesamt
Abwehr einer vom Betroffenen ausgehenden Gefährdung	181	2	-	183
Abwehr anderer erheblicher Gefahren für die innere oder äußere Sicherheit	122	500	2	624
Abwehr einer vom Betroffenen ausgehenden Gefährdung **und** Abwehr anderer erheblicher Gefahren für die innere oder äußere Sicherheit	10	-	-	10
Keine Angabe	1	-	-	1
Gesamt	**314**	**502**	**2**	**818**

Ausschreibungsgegenstände

Alle drei Nachrichtendienste setzten das Instrument in erster Linie dazu ein, um im SIS II *Personen* auszuschreiben (808 Fälle). Lediglich in sieben Fällen erfolgte eine Ausschreibung von *Fahrzeugen* durch das BfV. In drei Fällen wurden sowohl Personen als auch eine in Artikel 36 Abs. 1 des Beschlusses 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) genannte Sache ausgeschrieben. In den Fällen, in denen eine Sache ausgeschrieben wurde, handelte es sich um Fahrzeuge (7). In einem Fall wurden Fahrzeuge, Wasserfahrzeuge, Luftfahrzeuge und Container ausgeschrieben. Bei zwei Ausschreibungen wurden keine weiteren Angaben gemacht.

Treffermeldungen

Hinsichtlich der Ausschreibungstreffer zeigten sich deutliche Unterschiede zwischen BfV, BND und BAMAD: In rund der Hälfte der BfV-Ausschreibungen (157) wurde die ausgeschriebene Person angetroffen, während die andere Hälfte der Ausschreibungen (156) erfolglos blieb. Hingegen gab es bei den BND-Ausschreibungen vergleichsweise weniger Treffermeldungen. Nur in gut 26 Prozent der BND-Ausschreibungen wurden die ausgeschriebenen Personen angetroffen. Rund 74 Prozent der BND-Ausschreibungen ergaben hingegen keinen Treffer. Bei den BAMAD-Ausschreibungen wurde in einem Fall die ausgeschriebene Person angetroffenen, während es in dem anderen Fall keine Treffermeldung gab.
Das BfV wies darauf hin, dass die Ausschreibungsdauer von maximal sechs Monaten in der Regel ausgeschöpft werde, da es nicht absehbar sei, wann die Ausreise oder die Rückkehr zu erwarten sei. Zudem sei es für die Erstellung eines Bewegungsprofils hilfreich, mehrere Ein- und Ausreisen zu dokumentieren.

Tab. 12: Treffermeldungen im SIS II

Antreffen der ausgeschriebenen Person bzw. Sache	**BfV**	**BND**	**BAMAD**	**Gesamt**
Angetroffen	157	133	1	291
in %	*50,2 %*	*26,5 %*	*50 %*	*35,6 %*
Nicht angetroffen	156	369	1	526
in %	*49,8 %*	*73,5 %*	*50 %*	*64,4 %*
Gesamt	**313**[147]	**502**	**2**	**817**

Bezogen auf die 291 Ausschreibungen, in denen es Treffer gab, wurde die ausgeschriebene Person oder Sache in rund 93 Prozent der Fälle einmal angetroffen. In 7 Prozent der Fälle kam es zu Mehrfachtreffern, d. h. die ausgeschriebene Person oder Sache wurde im Ausschreibungszeitraum mehrfach angetroffen. Im Großteil der Fälle (14) gab es zwei Treffer, während die ausgeschriebene Person oder Sache in vier Fällen dreimal und in zwei Fällen viermal angetroffen wurde.
Die Treffermeldungen stammten beim BfV aus 21 europäischen Ländern, wobei der überwiegende Teil (160 Treffer) von deutschen Polizeibehörden stammte. Darüber hinaus wurden in nennenswertem Umfang Informationen zu einer ausgeschriebenen Person oder Sache aus Bulgarien (17) und Frankreich (11) übermittelt.
Bei den Ausschreibungen des BND zeigte sich ein ähnliches Bild. In 43 Fällen stammten die Informationen aus Deutschland. Zudem übermittelten spanische (22) und britische (10) Sicherheitsbehörden Informationen in einem nennenswerten Umfang.

[147] In einem Fall wurde eine Person im SIS II ausgeschrieben, die Rückmeldung erfolgte jedoch im Rahmen einer stillen Grenzfahndung nach § 17 Abs. 2 BVerfSchG, sodass die Angaben, die im Zusammenhang mit dem Antreffen der Person gemacht wurden, hier nicht weiter berücksichtigt wurden.

Tab. 13: Übermittlungen der SIS II-Informationen nach Ländern[148]

Übermittelndes Land	BfV	BND	BAMAD	Anzahl der Meldungen
Deutschland	116	43	1	160
Spanien	1	22	-	23
Bulgarien	17	3	-	20
Frankreich	11	5	-	16
Großbritannien	2	10	-	12
Schweiz	6	5	-	11
Norwegen	1	8	-	9
Belgien	1	7	-	8
Polen	4	3	-	7
Dänemark	2	4	-	6
Ungarn	5	1	-	6
Griechenland	4	2	-	6
Italien	1	4	-	5
Österreich	2	3	-	5
Rumnänien	1	4	-	5
Slowenien	4	1	-	5
Tschechien	2	3	-	5
Niederlande	3	1	-	4
Finnland	-	3	-	3
Schweden	1	2	-	3
Kroatien	1	-	-	1
Gesamt	**185**	**134**	**1**	**320**

[148] Da es bei neun Ausschreibungen zu Mehrfachtreffern gekommen ist, übersteigt die in der Tabelle angegebene Gesamtzahl die Anzahl der Ausschreibungen mit Treffern.

Art der übermittelten Informationen

Im Rahmen der Kontrollen wurden hauptsächlich Informationen zum Auffinden der ausgeschriebenen Person (285), zu Ort, Zeit oder Anlass der Kontrolle (275), sowie zum Reiseweg und -ziel (199) übermittelt. Des Weiteren erhielt die ausschreibende Behörde Informationen zum benutzten Fahrzeug, Wasserfahrzeug, Luftfahrzeug oder benutzten Container (193), zu Begleitpersonen, bei denen begründeterweise davon ausgegangen werden kann, dass sie mit den betreffenden Personen in Verbindung stehen (175), zu mitgeführten Sachen (27) sowie zu den Umständen des Auffindens der Person (29).
Bei den sechs Ausschreibungen des BND – hierbei handelte es sich um sechs unterschiedliche Personen, zu denen der BND teilweise mehrfache Treffer verzeichnete – wurden Informationen zum Auffinden der ausgeschriebenen Person (6), zu Ort, Zeit oder Anlass der Kontrolle (6), zum Reiseweg und -ziel (5), zum benutzen Fahrzeug, Wasserfahrzeug, Luftfahrzeug oder benutzter Container (4) sowie zu Begleitpersonen, bei denen begründeterweise davon ausgegangen werden kann, dass sie mit den betreffenden Personen in Verbindung stehen (3), übermittelt.

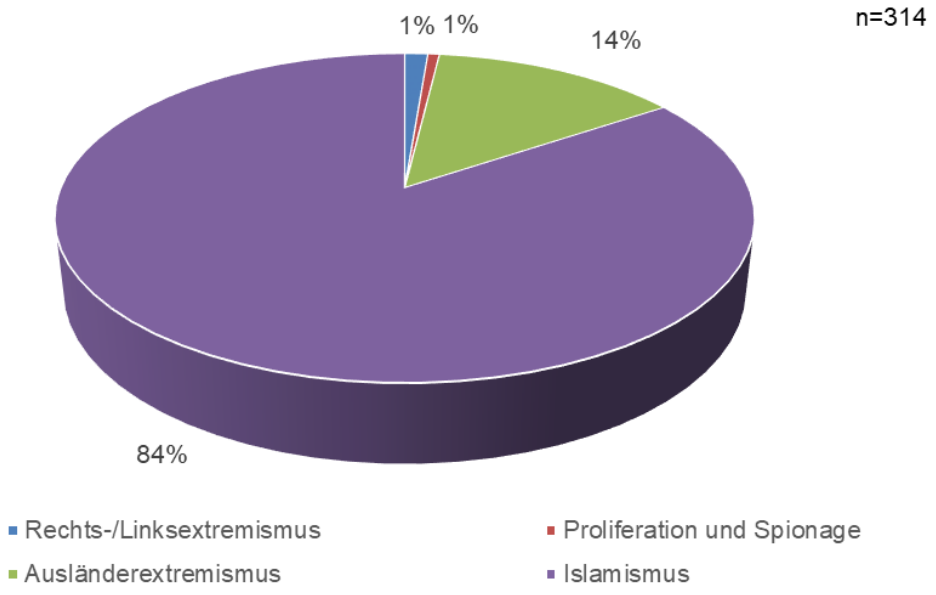
Tab. 14: Art der bei den Zufallskontrollen übermittelten Informationen

Art der übermittelten Informationen	**BfV (n=157)**	**BND (n=133)**	**BAMAD (n=1)**	**Gesamt (n=291)**
Ort, Zeit oder Anlass der Kontrolle	143	131	1	275
Auffinden der Person	151	133	1	285
Reiseweg und -ziel	100	98	1	199
Begleitpersonen	98	77	-	175
Benutztes Fahrzeug, Wasserfahrzeug, Luftfahrzeug oder benutzter Container	82	110	1	193
Umstände des Auffindens der Person	56	16	-	72
Mitgeführte Sachen	93	28	-	121
Gesamt	**723**	**593**	**4**	**1.320**

Phänomenbereiche

In den allermeisten Fällen nutzte das BfV die Möglichkeit gemäß § 17 Abs. 3 BVerfSchG dazu, Informationen über Personen bzw. Sachen im Bereich Islamismus (265) bzw. Ausländerextremismus (43) zu gewinnen. Eine untergeordnete Rolle spielten dagegen die Bereiche Proliferation und Spionage (2) sowie Rechts- und Linksextremismus (4).

Abb. 6: SIS II-Ausschreibungen nach Phänomenbereichen[149]



Befristung, Verlängerung und Löschung der Ausschreibungen

Hinsichtlich der Ausschreibungspraxis ist festzustellen, dass bei fast allen Ausschreibungen der drei Nachrichtendienste im Erhebungszeitraum die maximale Befristungsdauer von sechs Monaten ausgeschöpft wurde. In lediglich einem Fall wurde die Ausschreibung auf 22 Tage befristet. In einem anderen Fall wurden hierzu keine Angaben gemacht. In etwa acht von zehn Fällen kam es zu einer wiederholten Anordnung der Ausschreibung, wobei dies in 87 Prozent der Fälle zwischen ein- und fünfmal geschah. Etwa 13 Prozent der Ausschreibungen wurden zwischen sechs- und zehnmal angeordnet, während es in zwei Fällen zu elf- bzw. vierzehnmaligen Anordnungen der Ausschreibung kam.
Angaben zu den Gründen für die Löschung der SIS II-Ausschreibungen wurden in 328 Fällen gemacht. In 195 Fällen lagen die Voraussetzungen für die Ausschreibung nicht mehr vor. Bei 80 Ausschreibungen habe sich gezeigt, dass der Zweck der Maßnahme nicht erreicht werden konnte. In 36 Fällen wurde angegeben, dass der Zweck der Maßnahme erreicht werden konnte. Bei 14 Ausschreibungen wurde vom BfV als Grund für die Löschung der Maßnahme genannt, dass die Voraussetzungen für die Ausschreibung nicht mehr vorlagen und der Zweck der Maßnahme erreicht wurde. In drei Fällen wurde darauf hingewiesen, dass die Voraussetzung für die Maßnahme nicht mehr vorlagen und dass der Zweck der Maßnahme nicht erreicht werden konnte. Zu 490 Ausschreibungen wurden keine Angaben zu den Löschungsgründen gemacht, da die Ausschreibungen größtenteils noch nicht gelöscht worden waren.

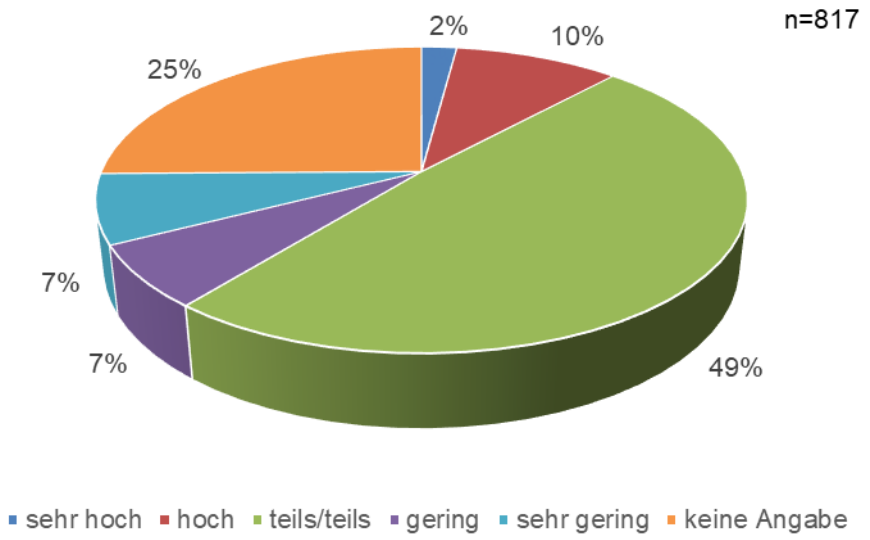
Nutzen der gewonnenen Informationen für die nachrichtendienstliche Arbeit

Die Bewertung der im Rahmen der Ausschreibung gewonnenen Informationen für die nachrichtendienstliche Arbeit fiel insgesamt divers aus. In rund zwölf Prozent der Ausschreibungen wurde der Nutzen der gewonnenen Informationen als hoch bzw. sehr hoch eingeschätzt. In etwa knapp der Hälfte der Fälle waren die Informationen zumindest teilweise von Nutzen. In etwa 14 Prozent der Fälle wurde ihr Nutzen als gering bzw. sehr gering bewertet. Zu 206

[149] Zu den Ausschreibungen vom BND und BAMAD wurden keine Informationen zu den Phänomenbereichen erhoben.

Ausschreibungen wurden keine Angaben zur Nutzenbewertung von den drei Nachrichtendiensten gemacht. Bei diesen Fällen handelte es sich fast ausschließlich um Ausschreibungen des BND (204).

Abb. 7: Bewertung der im Rahmen der SIS II-Ausschreibung gewonnenen Informationen für die nachrichtendienstliche Arbeit



Die genauen Begründungen für die jeweilige Nutzenbewertung sind im Anhang (S. 163 ff.) aufgeführt.

Bei einer differenzierten Analyse der Ergebnisse zeigte sich ein großer Unterschied hinsichtlich der Nutzenbewertung sowohl zwischen BfV/BAMAD und BND als auch zwischen Ausschreibungen, in denen Informationen zu der ausgeschriebenen Person bzw. Sache übermittelt wurden, und Ausschreibungen, die zu keinem Treffer führten. Für die Gruppe der Ausschreibungen mit Treffermeldung wurde der Nutzen der gewonnenen Informationen in knapp 50 Prozent der Fälle vom *BfV/BAMAD* als hoch bzw. sehr hoch bewertet. In rund 46 Prozent der Ausschreibungen wurden die übermittelten Informationen als teilweise nützlich eingestuft. In rund vier Prozent der Fälle wurde der Nutzen als gering eingeschätzt.

Der *BND* bewertete hingegen den Nutzen aller im Rahmen der SIS II-Ausschreibung gewonnenen Informationen, die aus einer Treffermeldung stammten, als teilweise nützlich.

Bei den Ausschreibungen, die zu keinem Treffer führten, fiel die Nutzenbewertung deutlich schlechter aus. In etwas mehr als vier Prozent der Fälle wurde der Nutzen vom *BfV/BAMAD* als hoch bzw. sehr hoch bewertet. In rund 26 Prozent der Fälle waren die im Rahmen der Ausschreibung gewonnenen Informationen teilweise von Nutzen. Bei etwa 68 Prozent der Ausschreibungen wurde der Nutzen als gering bzw. sehr gering eingestuft. In etwas mehr als einem Prozent der Fälle wurden keine Angaben zur Nutzenbewertung gemacht.

Der *BND* bewertete den Nutzen der Informationen, die aus SIS II-Ausschreibungen ohne Treffermeldung stammten, in nur rund drei Prozent der Fälle als hoch. In mehr als 41 Prozent waren die Informationen teilweise von Nutzen, während zu mehr als 55 Prozent der Ausschreibungen keine Angaben gemacht wurden. Letzteres erklärte der BND damit, dass für ihn als Auslandsnachrichtendienst mit Fokus auf bestimmte Zielregionen außerhalb des Schengen-Raumes fehlende Treffer für Ausschreibungen aus dem Schengen-Raum oftmals keine inhaltlich verwertbaren Rückschlüsse zulassen.

Bewertung und Optimierungsbedarf aus Sicht der Nachrichtendienste

Die Ergebnisse der Analyse verdeutlichen, dass mit einer SIS II-Ausschreibung – im Falle eines Treffers – für die nachrichtendienstliche Arbeit durchaus wichtige Informationen gewonnen werden können. Im Einzelfall kann aber auch der Nicht-Treffer einen hohen Informationsgehalt aufweisen.

Beim BND fiel die Bewertung hingegen sowohl bei erzielten Treffern als auch keinen Treffern insgesamt eher verhalten aus, da in mehr als der Hälfte der Fälle (286) der Nutzen der im Rahmen der Ausschreibung gewonnenen Informationen für die nachrichtendienstliche Arbeit nur teilweise von Nutzen waren. Begründet wurde die Einschätzung damit, dass durch die Ausschreibung Informationen zu Reisebewegungen der betreffenden Personen gewonnen werden konnten, die zur Erfüllung des Auftrags der Abteilung TE des BND auf dem Gebiet der Aufklärung des internationalen Terrorismus beigetragen haben. In 204 Fällen, in denen keine Angaben zur Nutzenbewertung gemacht wurden, begründete der BND dies damit, dass im Erhebungszeitraum kein Treffer angefallen war. In zwölf Fällen wurde – obwohl es keine Treffermeldung gegeben hat – der Nutzen der gewonnenen Informationen als hoch eingeschätzt. Als Grund wurde hierfür angeführt, dass der BND sich von der Ausschreibung künftig wichtige Erkenntnisse zum Reiseverhalten der ausgeschriebenen Person erhoffe.

Das BfV und der BND plädierten dafür, das Instrument der SIS II-Ausschreibung beizubehalten, da es eine sehr gute Möglichkeit darstelle, Reisebewegungen feststellen und Routen von Kurieren, Nachrichtenmittlern und Rekrutieren nachzeichnen sowie um Organisationsstrukturen aufdecken zu können.

Auch aus Sicht des BAMAD sei die SIS II-Ausschreibung eine wichtige Maßnahme zur Informationsgewinnung.

Nach Ansicht des BfV sei es jedoch sinnvoll, den Ausschreibungszeitraum von sechs auf zwölf Monate zu verlängern, da dies eher den üblichen Bewegungsmustern entspräche. Erkennbar sei dies auch daran, dass es in der Praxis kaum Ausschreibungen gebe, die nicht verlängert würden. Auch sei dies vom EU-Ratsbeschluss gedeckt und werde von anderen EU-Mitgliedstaaten bereits praktiziert. Eine Verlängerung der Ausschreibungsfrist würde zudem zu einer Reduzierung des Aufwandes für das BfV führen. Aus Sicht des BAMAD sei es zudem wünschenswert, die Hürden für die Beantragung einer solchen Maßnahme, die bereits von den Anforderungen her in den strafrechtlichen Bereich hineinreichen würden, abzusenken, da sie die einzige Möglichkeit darstelle, Reiseaktivitäten festzustellen. Anders als beim BfV werde der Ausschreibungszeitraum von sechs Monaten jedoch als ausreichend angesehen, da es bisher keinen Fall gegeben habe, in dem eine Ausschreibung verlängert werden musste.

Der BND merkte an, dass durch die Einstellung in die Nationale Sirene die Zielperson ‚markiert' und damit der Blick ausländischer Nachrichtendienste auf ein deutsches nachrichtendienstliches Interesse an der Person – ggf. indirekt auf deren Quelleneigenschaft – gelenkt werden könne. Deshalb bestehe ein praktisches Bedürfnis, den nachrichtendienstlichen Hintergrund der Ausschreibung verschleiern zu können. Zudem würde dies einen Betroffenen vor weiteren Maßnahmen anderer Nachrichtendienste schützen, die im Einzelfall durch ausländische Nachrichtendienste wegen des – für mit der Materie vertraute Personen – erkennbaren deutschen nachrichtendienstlichen Interesses ergriffen würden. Des Weiteren sei es wünschenswert, dass die Rückmeldung durch die Polizei vor Ort schneller erfolge. Ein Problem stelle darüber hinaus die Aushebelung von SIS II-Ausschreibungen durch die Nutzung falscher Ausweispapiere dar, weshalb aus Sicht des BND eine Biometrisierung des Reisepasses hilfreich wäre.

Zusammenfassend ist festzuhalten, dass die SIS II-Ausschreibungen gemäß § 17 Abs. 3 BVerfSchG aus Sicht der Nachrichtendienste ein wichtiges Instrument für die Erstellung von

Reiseprofilen darstellen, das im Erhebungszeitraum in erster Linie vom BfV und vom BND genutzt wurde. Aufgrund der sicherheitspolitischen Lage wurde von dieser Möglichkeit – im Vergleich zur vorherigen Evaluation – dieses Mal deutlich häufiger Gebrauch gemacht. In knapp zwei Drittel der Fälle erfolgte trotz wiederholter Ausschreibung keine Treffermeldung, wobei die Trefferquote des BfV/BAMAD deutlich höher als die des BND war. Jedoch kann auch diese Tatsache eine für die Nachrichtendienste wichtige und wertvolle Information sein. Zudem handele es sich bei den Kontrollen strukturell nicht um ein gezieltes Feststellen einer Person, sondern letztlich um ein zufälliges Antreffen im Rahmen von Routinekontrollen. Folglich sei es hier schwer, eine hohe Effektivität des Instruments dadurch zu belegen, dass höhere Trefferquoten erzielt werden.

4.5.3. Rechtswissenschaftliche Bewertung

Hinsichtlich der verfassungsrechtlichen Bewertung der empirisch erhobenen Praxis der Ausschreibung nach § 17 Abs. 3 BVerfSchG, Art. 36, 37 des Beschlusses 2007/533/JI des Rates vom 12. 6. 2007 ist hinsichtlich der Geeignetheit darauf hinzuweisen, dass Ausschreibungen des BfV/BAMAD zu etwa 50 Prozent und Ausschreibungen des BND zu etwa 26 Prozent zu Treffern führten. Zudem wird für einen signifikanten Anteil der Ausschreibungen zumindest ein teilweiser Nutzen angegeben (12 Prozent sehr hoch oder hoch, 49 Prozent teils/teils). Zweifel an der Geeignetheit bestehen demnach nicht. Ein milderes Mittel, diese Ziele gleich wirksam zu erreichen, ist insbesondere für die Gewinnung von Informationen aus dem europäischen Ausland nicht erkennbar.

Für die Bewertung der Einhaltung der durch das Gebot der Verhältnismäßigkeit im engeren Sinne gezogenen Grenzen ist zunächst zu beachten, dass § 17 Abs. 3 S. 1 BVerfSchG, Art. 36 Abs. 3 Beschluss 2007/533/JI ein hohes Gefährdungspotential für hochrangige Rechtsgüter auf der Grundlage konkreter Informationen voraussetzt. Andererseits ist der mit der Maßnahme verbundene Eingriff zu gewichten. Durch die Abfrage sollen Reisewege und damit grobe Bewegungsprofile nachgezeichnet werden. Damit liegt ein Eingriff in die informationelle Selbstbestimmung von eher geringer Tiefe vor. Zudem enthält § 17 Abs. 3 BVerfSchG eine Austarierung der Eröffnung von Grundrechtseingriffen mit materiellen und verfahrensmäßigen Sicherungen zum Grundrechtsschutz. Zu diesen Sicherungen durch Verfahren zählt auch die grundsätzliche Befristung der Ausschreibung auf höchstens sechs Monate durch § 17 Abs. 3 S. 4 BVerfSchG. Wenngleich die Vorschrift vorsieht, dass die Ausschreibung auch wiederholt angeordnet werden kann, ist damit zum Ausdruck gebracht, dass die Ausschreibung grundsätzlich kein Instrument einer Informationsbeschaffung in Permanenz ist. Gleichwohl sind die Ausschreibungen in etwa 80 Prozent der Fälle wiederholt beantragt worden. Dies hat dazu geführt, dass Ausschreibungen teilweise über mehrere Jahre liefen. Diese Tatsache indiziert für sich noch keine unangemessene, flächenhafte Anwendung, da die Verlängerung immer eine Einzelfallentscheidung ist und die veränderten Sicherheitslagen und Reisebewegungen gerade im Bereich des islamistischen Terrorismus durchaus längerfristige Ausschreibungen nahelegen. Dies macht zudem den Anstieg in der Nutzung des Instruments plausibel.

Jedoch stellt die nicht unerhebliche Zahl an Nicht-Treffern und der teils geringe Nutzen (14 Prozent geringer bzw. sehr geringer Nutzen gegenüber 12 Prozent sehr hoher bzw. hoher Nutzen) insofern eine rechtliche Herausforderung dar, als dass eine Ausschreibung auch dann, wenn sie zu keinem Treffer führt, durch die (indirekte) „Markierungswirkung“ ein besonderes Interesse ausländischer Nachrichtendienste an der Zielperson auslösen und sie damit als mögliche Quelle unbrauchbar machen und sie auch faktisch belasten kann. Dies

sollte zum Anlass genommen werden, die vom BND erwogene Verschleierung des nachrichtendienstlichen Hintergrundes auf ihre rechtliche und technische Realisierbarkeit zu prüfen.

4.6. § 18 Abs. 1a BVerfSchG

4.6.1. Genese der Regelungen

Die Vorschrift regelt die Pflicht zur Initiativübermittlung von einschlägigen Daten durch das BAMF an das BfV bzw. der Ausländerbehörden eines Landes an die Verfassungsschutzbehörden eines Landes (sog. Spontanübermittlung). Die Datenübermittlung des BAMF an das BfV richtet sich im Übrigen nach § 73 Abs. 1 und § 73a Aufenthaltsgesetz (AufenthG), die eine Pflicht zur Übermittlung allerdings nicht vorsehen.
Die Bestimmung wurde mit dem TBG im Jahre 2002 neu eingeführt.[150] Die Gesetzesbegründung verwies auf die UN-Resolution 1373 (2001).[151] Danach sollen die Mitgliedstaaten, bevor sie einer Person Flüchtlingsstatus gewähren, geeignete Maßnahmen ergreifen, um sich zu vergewissern, dass der Asylsuchende keine terroristischen Handlungen geplant oder erleichtert oder sich daran beteiligt hat.[152] Bis zum TBEG hatte Satz 2 den Wortlaut: „Die Übermittlung dieser personenbezogenen Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen nach § 19 Abs. 3 BVerfSchG unterbleibt, es sei denn, die Übermittlung ist völkerrechtlich geboten.“ Mit dem TBEG 2007 erhielten § 18 Abs. 1a S. 1, 2 BVerfSchG die bis heute bestehende Formulierung. Die Vorschrift wurde zudem um die Sätze 3 und 4 erweitert.[153] Im Jahre 2011 wurde die Bestimmung um einen Satz 5 ergänzt.[154]

4.6.2. Empirische Ergebnisse

Durch das TBG wurde § 18 Abs. 1a BVerfSchG eingefügt und damit die erweiterte Pflicht für das BAMF geschaffen, unter bestimmten Voraussetzungen Informationen an das BfV zu übermitteln. Diese Informationen sollen dazu dienen, einen Überblick über die mögliche Entwicklung von Ablegern islamistischer gewaltbereiter Organisationen, die terroristische Aktivitäten im Inland planen, zu gewinnen. Da § 18 Abs. 1 BVerfSchG lediglich eine Übermittlung des BAMF an das BfV, jedoch unter erhöhten Anforderungen, ermöglicht hatte und eine Übermittlungspflicht für die Ausländerbehörden der Länder an die Verfassungsschutzbehörden der Länder bislang nicht existierte, schloss der Gesetzgeber mit § 18 Abs. 1a BVerfSchG eine Regelungslücke.[155] Eine entsprechende Regelung zur Übermittlung von Informationen durch das BAMF an den BND und an das BAMAD existiert im BNDG und MADG nicht. Durch das Gesetz zur Änderung des Bundesverfassungsschutzgesetzes vom 7. Dezember 2011 wurde der bisherigen Regelung der Satz 4 hinzugefügt, der vorsieht, dass die Zuständigkeit und das Verfahren für die Entscheidung des BAMF zu Übermittlungen nach Satz 1 in einer Dienstvorschrift zu regeln sind, die der Zustimmung des BMI bedarf.
Die Zuständigkeit und das Verfahren für die Entscheidung des BAMF zu Übermittlungen gemäß § 18 Abs. 1a S. 1 BVerfSchG ist in der Dienstanweisung Sicherheit (DA-Sicherheit),

---

[150] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 363, in Kraft getreten am 01.01.2002.
[151] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 41.
[152] Vgl. Resolution 1373 (2001) vom 28.09.2001, Ziffer 3f), abrufbar unter: http://www.un.org/depts/-german/sr/sr_01-02/sr1373.pdf.
[153] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 4, in Kraft getreten am 11.01.2007.
[154] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2578, in Kraft getreten am 10.01.2012.
[155] Vgl. BT-Drs. 14/7386 (neu), S. 41.

die Bestandteil der Dienstanweisung Asylverfahren (DA-Asyl) ist, geregelt. Für die Übermittlung von Informationen aus dem Asylverfahren an die Sicherheitsbehörden ist im BAMF das Referat 241 „Operative Zusammenarbeit mit den Sicherheitsbehörden des Bundes und der Länder“ als zentrale Stelle zuständig.
Des Weiteren enthält die DA-Sicherheit Erläuterungen zum Vorgehen bei Übermittlungen nach anderen Vorschriften (gemäß § 18 Abs. 1 und 3 BVerfSchG, § 10 Abs. 1 und 2 MADG, § 23 Abs. 1 BNDG, § 8 Abs. 3 AsylG sowie § 20x BKAG) sowie einen gemeinsamen Kriterienkatalog, der als Entscheidungshilfe für die Datenübermittlung des BAMF an das BfV gemäß § 18 Abs. 1 und 1a BVerfSchG sowie an den BND gemäß § 23 Abs. 1 BNDG dient. Für das BAMAD existiert kein eigener Kriterienkatalog. Der gemeinsame Kriterienkatalog von BfV und BND umfasst in der Langfassung 67 Seiten (Stand: August 2017) und besteht aus einem allgemeinen Kriterienteil und einem länderspezifischen Teil. In der DA-Sicherheit sind zudem ausgewählte Kriterien zu finden, die vor der Übermittlung von Informationen an das Sicherheitsreferat im BAMF (Referat 241) herangezogen werden. Dort ist festgelegt, dass die Mitarbeiterinnen und Mitarbeiter in den Außenstellen Informationen, die gemäß Kriterienkatalog sicherheitsrelevant sein können, mittels einer in Outlook hinterlegten E-Mail-Vorlage (seit Sommer 2017 verfügbar) umgehend an das Referat 241 zu übermitteln haben. Dieses prüft, ob die Kriterien zur Übermittlung erfüllt sind und leitet die Informationen an die zuständigen Sicherheitsbehörden weiter. Die Bewertung, ob relevante Informationen vorliegen, übernimmt seit der Anwendung des gemeinsamen Kriterienkatalogs nicht mehr das Referat 241, sondern wird durch die Anhörer vor Ort sowie durch die Nachrichtendienste, welche die Informationen erhalten, geleistet.
Im Rahmen der neuen DA-Sicherheit wurde zudem mit dem Sonderbeauftragten für Sicherheit im Asylverfahren eine neue Stelle in den Außenstellen geschaffen, die als zentraler Ansprechpartner für Fragen und Probleme mit sicherheitsrelevantem Hintergrund fungiert.
Im Erhebungszeitraum hat es im Vergleich zur vorherigen Evaluation 24-mal mehr Übermittlungen gemäß § 18 Abs. 1a BVerfSchG gegeben, sodass eine Anpassung des Datenerhebungsverfahrens erforderlich wurde. Aufgrund der Vielzahl von Spontanübermittlungen konnte das BfV nicht für jede Übermittlung einen Erhebungsbogen ausfüllen. Um jedoch quantitative Aussagen zu den im Evaluationszeitraum vom BAMF übermittelten Informationen treffen zu können, stellte das BfV die Gesamtzahl der Spontanübermittlungen sowie der vom BfV gespeicherten Informationen differenziert nach Abteilungen zur Verfügung. Dadurch war es jedoch für das BfV nicht möglich, für jede Übermittlung des BAMF einzelfallbezogene Angaben (z. B. zur Art der gespeicherten personenbezogenen Daten oder zum Erkenntniswert der einzelnen vom BAMF übermittelten Informationen) zu machen.
Wurden im Jahr 2013/14 vom BAMF in insgesamt 200 Fällen Informationen ans BfV übermittelt, waren es im Jahr 2016/17 4.787 Übermittlungen, die vom BfV abschließend bearbeitet werden konnten. Der Großteil der vom BAMF übermittelten Informationen (80 Prozent) hatte Islamismusbezüge und ging daher an die Abteilung 6. Bei etwas mehr als 16 Prozent der Fälle gab es Hinweise auf Ausländerextremismus, sodass die Übermittlungen von der Abteilung 5 bearbeitet wurden. Eine untergeordnete Rolle mit einem Anteil von drei Prozent spielten hingegen die Übermittlungen mit Bezug zu Proliferation und Spionagetätigkeiten, die an die Abteilung 4 gingen.

Tab. 15: Anzahl der Übermittlungen gemäß § 18 Abs. 1a BVerfSchG nach Abteilungen des BfV

Abteilungen BfV	1.10.-30.11.2016	1.12.2016-30.4.2017	1.5.-30.9.2017	Gesamt	In %
Spionageabwehr und Proliferation (Abteilung 4)	-	85	58	143	3,0
Ausländer- und Links-extremismus (Abteilung 5)	53	210	530	793	16,6
Islamismus und islamistischer Terrorismus (Abteilung 6)	574	1.889	1.388	3.851	80,4
BfV gesamt	**627**	**2.184**	**1.976**	**4.787**	**100,0**

Hinsichtlich der Speicherquote zeigten sich ebenfalls deutliche Unterschiede. Führte 2013/14 nur jede fünfte Übermittlung des BAMF zu einer Speicherung von Informationen beim BfV, war dies im Erhebungszeitraum bei vier von fünf Übermittlungen der Fall. Bei einer differenzierteren Betrachtung wurde zudem deutlich, dass es auch große Unterschiede zwischen den Speicherquoten der einzelnen Abteilungen im BfV gab. Während die Abteilung 6 knapp 90 Prozent der übermittelten Informationen speicherte, war dies in Abteilung 4 nur in knapp sieben Prozent der Fall. Von Abteilung 5 wurden mehr als 40 Prozent der vom BAMF übermittelten Informationen gespeichert.

Tab. 16: Anzahl der Speicherungen nach Abteilungen des BfV (absolut und in %)

Abteilungen BfV	Anzahl der Übermittlungen	Anzahl der Speicherungen	In % Abteilung	Gesamt	In % gesamt
Spionageabwehr und Proliferation (Abteilung 4)	143	5	3,5	143	3,0
Ausländer- und Linksextremis-mus (Abteilung 5)	793	326	41,1	793	16,6
Islamismus und islamistischer Terrorismus (Abteilung 6)	3.851	3.402	88,3	3.851	80,4
Gesamt	**4.787**	**3.733**	**78,0**	**4.787**	**100,0**

Eine einzelfallbezogene Erfassung, welche personenbezogenen Daten vom BfV gespeichert wurden, sowie eine einzelfallbezogene Bewertung des Nutzens für die nachrichtendienstliche Arbeit waren nicht möglich, da aufgrund der Vielzahl von BAMF-Übermittlungen im

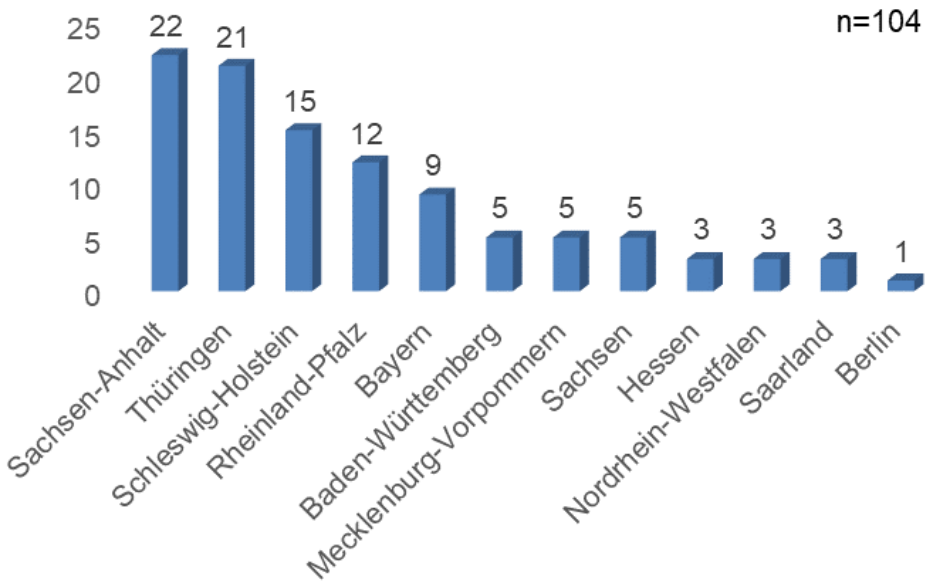
Evaluationszeitraum von einer Einzelfallerfassung auf eine aggregierte Datenerhebung mittels NADIS WN umgestellt werden musste.
Im Evaluationszeitraum übermittelten die Abteilungen 4 und 5 des BfV keine BAMF-Informationen an andere ausländische öffentliche Stellen bzw. zwischen- oder überstaatliche Stellen. Die Abteilung 6 wies darauf hin, dass sie hierzu keine konkreten Angaben machen könne, gab aber an, dass die Zahl der Fälle, in denen eine Übermittlung an andere ausländische öffentliche Stellen bzw. zwischen- oder überstaatliche Stellen erfolge, gegenwärtig bei unter einem Prozent liege. Hierbei habe es sich um ausländische Partnerdienste gehandelt.
Auffällig ist, dass die Zahlen im Evaluationszeitraum sich deutlich von den Evaluationen aus den Jahren 2009 sowie 2013/14 unterscheiden. So wurden deutlich mehr Informationen vom BAMF an das BfV übermittelt (2009: 648; 2013/2014: 200, 2016/17: 4.787). Gleichzeitig erhöhte sich der Anteil der Informationen deutlich, die vom BfV gespeichert wurden (2009: 12,5 Prozent; 2013/2014: 20 Prozent; 2016/17: 78 Prozent).
Von Seiten des BAMF wurde die hohe Zahl an Spontanübermittlungen damit begründet, dass der islamistische Terrorismus mit dem Aufkommen des Islamischen Staates stark an Bedeutung gewonnen habe und aufgrund der in Deutschland angespannten Sicherheitslage vor allem die Sensibilität der Mitarbeiterinnen und Mitarbeiter des BAMF vor Ort größer geworden sei. Dies sei auch darauf zurückzuführen, dass in den letzten Jahren eine Vielzahl neuer Mitarbeiterinnen und Mitarbeiter eingestellt worden sei, die noch keine langjährigen Routinen entwickelt hätten, und regelmäßig Vor-Ort-Schulungen des Sicherheitsreferats in Zusammenarbeit mit den Verbindungsbeamten des BND und des BfV durchgeführt würden, sodass das Instrument der Spontanübermittlung frühzeitig bekannt und implementiert würde.
Aus Sicht des BAMF sei die Möglichkeit, Informationen gemäß § 18 Abs.1a BVerfSchG ans BfV zu übermitteln, – insbesondere angesichts der derzeit angespannten Sicherheitslage in Deutschland – sehr wichtig. Vor allem die BAMF-Übermittlungen mit Hinweisen auf Extremismus, Terrorismus und Radikalisierungen hätten in den letzten Jahren eine große Rolle gespielt. Gerade bei Radikalisierungstendenzen lägen oft aber keine klaren Beweise vor, sodass eine Übermittlung nach § 18 Abs. 1 BVerfSchG als Alternative nicht in Frage käme. Das Referat 241 sah kaum Optimierungsbedarf im Bereich der Spontanübermittlungen. Es wurde lediglich angeregt, eine vergleichbare Möglichkeit zur direkten Übermittlung von Informationen an das BAMAD zu schaffen, da dies derzeit unter Verweis auf § 10 Abs. 1 MADG mit höheren Anforderungen verbunden sei und eine Übermittlung vom BAMF über das BfV an das BAMAD als umständlich angesehen werde.
Das BfV stellte mit Blick auf die deutliche Zunahme der Spontanübermittlungen des BAMF fest, dass die Informationen dort insgesamt weniger gefiltert würden. Seit der Flüchtlingskrise scheine das BAMF bei seinen Übermittlungen „auf Nummer sich zu gehen“, da möglicherweise vermieden werden solle, dass relevante Informationen nicht an die Nachrichtendienste weitergeleitet würden. Mit Blick auf die Zusammenarbeit mit dem BAMF monierte das BfV, dass die übermittelten Dokumente in schlechter Qualität und nicht maschinenlesbar eingescannt seien. Zudem fehle noch eine standardisierte Vorlage für die Übermittlung vom BAMF ans BfV. Hieran werde aber derzeit gearbeitet.
Aus Sicht des BfV seien die Ersthinweise des BAMF für die nachrichtendienstliche Arbeit von großer Bedeutung, um relevante Informationen zu möglichen Gefährdern zu erhalten, die beispielsweise die Ziele des IS in Deutschland weiterverfolgen wollen. Verbesserungen seien nach Auffassung des BfV vor allem in organisatorischer Hinsicht wünschenswert. So wäre es hilfreich, wenn die Daten vom BAMF so übermittelt würden, dass sie vom BfV elektronisch weiterverarbeitet werden können. Darüber hinaus wäre eine intensivere Vorprüfung seitens des BAMF wünschenswert, um die Arbeit des BfV zu erleichtern. Des Weiteren gebe es

Optimierungspotenzial bei der Regelung zur erforderlichen Zustimmung des BAMF vor der Übermittlung an ausländische Partnerdienste. Diese sei nicht funktional, da zum einen das BfV dem BAMF aufgrund der VS-Einstufung wesentlicher Teile nur einen Teil der Informationen zur Verfügung stellen könne, die dieses für eine fundierte Entscheidung brauche. Zum anderen sei § 19 Abs. 3 BVerfSchG aus Sicht des BfV für solche Übermittlungen eine ausreichende Grundlage, da auch dort selbstverständlich die Belange des Betroffenen berücksichtigt würden. Die Überarbeitung des Kriterienkatalogs sei notwendig geworden, da der alte zu lang, komplex und unübersichtlich geworden wäre, um die Anhörerinnen und Anhörer in die Lage zu versetzen, relevante Informationen zu erkennen und gezielt nachzufragen. Die unterschiedliche Verteilung der Spontanübermittlungen auf die einzelnen Abteilungen des BfV wurde so erklärt, dass der Großteil der Flüchtlinge aus Ländern stammte, in denen der IS und/oder Jihadisten aktiv seien. Für diesen Bereich sei die Abteilung 6 zuständig, die die meisten Übermittlungen im Erhebungszeitraum erhalten habe.
Insgesamt kann festgehalten werden, dass das BAMF von seiner Möglichkeit, Informationen spontan an das BfV zu übermitteln, im Erhebungszeitraum intensiv Gebrauch machte. Dabei kam es sehr oft zu einer Speicherung von Informationen beim BfV. Aus Sicht des BAMF funktioniere die Zusammenarbeit mit den Sicherheitsbehörden sehr gut. Dies läge u. a. auch daran, dass Verbindungsbeamte des BND und BfV im BAMF säßen und aufgrund der hohen Priorität, die das Thema Sicherheit aktuell habe, auf allen Ebenen Kontakte zwischen dem BAMF und den Nachrichtendiensten bestünden.

Spontanübermittlungen von Ausländerbehörden der Länder

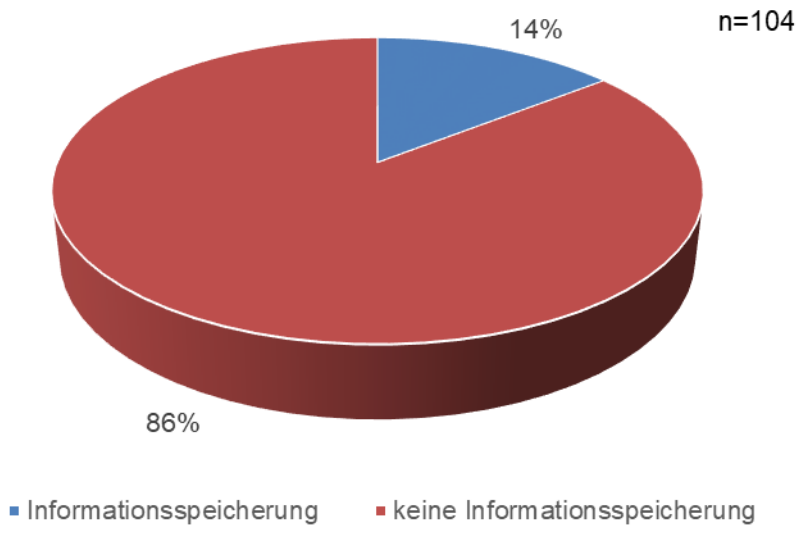
Im Gegensatz zum BAMF wurden von den Ausländerbehörden der Länder im Erhebungszeitraum nur vereinzelt Informationen gemäß § 18 Abs. 1a BVerfSchG an die Landesverfassungsschutzbehörden übermittelt. In 12 Bundesländern kam es in insgesamt 104 Fällen zu einer Spontanübermittlung von Informationen durch die Ausländerbehörden. Im Vergleich zur vorherigen Evaluation (2013/14: 33) kam es somit auch auf Bundesländerebene zu einem deutlichen Anstieg (2016/17: 104) – wenn auch nicht so stark wie beim Bund und auf einem insgesamt niedrigeren Niveau.

Abb. 8: Spontanübermittlungen der Ausländer- an die Landesverfassungsschutzbehörden



Hinsichtlich des Speicherverhaltens ergab sich auf Bundesländerebene ein komplett anderes Bild als auf Bundesebene. So wurden lediglich in etwas mehr als 14 Prozent der Fälle von den Ausländerbehörden übermittelte Informationen von den Landesverfassungsschutzbehörden gespeichert, während in knapp 86 Prozent der Fälle keine Speicherung erfolgte. Diese Quote war somit auch deutlich niedriger als bei der letzten Evaluation (2013/14: 27 Prozent).

Abb. 9: Umgang mit den von den Ausländerbehörden übermittelten Informationen



In den 15 Fällen[156] wurden von sieben Landesverfassungsschutzbehörden folgende Informationen gespeichert:

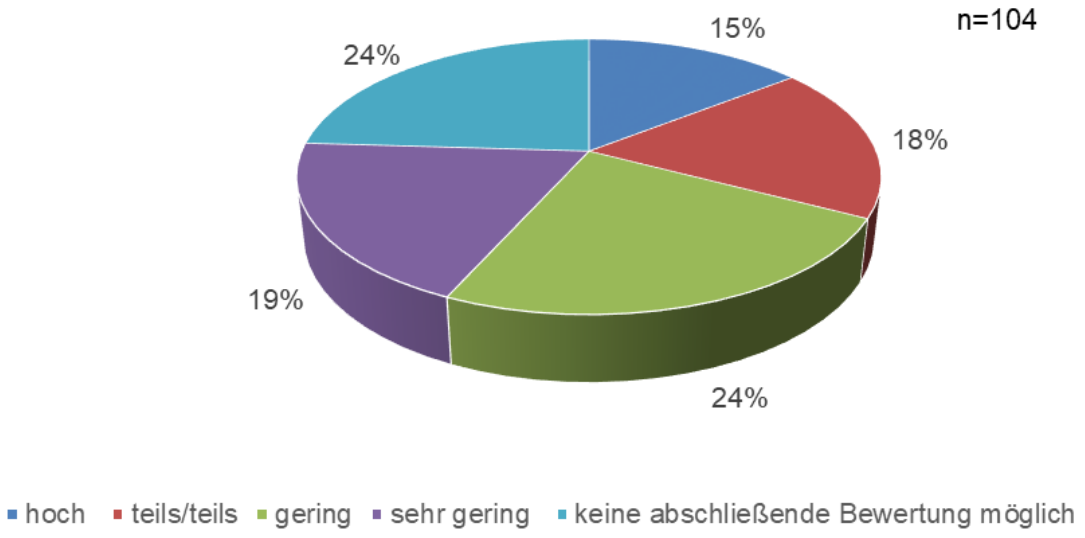
- Diverse Hinweise (z. B. Änderung des Erscheinungsbildes oder Verhaltens von Personen)
- Ein syrischer Flüchtling scheint labil zu sein und möchte wieder zurück nach Syrien. Er lehnt alle staatlichen Maßnahmen ab. Auch andere Syrer möchten keinen Kontakt, da sie ihn für gefährlich halten.
- Erkenntnisse über Aktivitäten von FND der GUS-Staaten gegen Asylbewerber in Deutschland
- Hinweis auf eine Kontaktperson
- Hinweis auf einen möglichen IS-Kämpfer unter einreisenden Flüchtlingen
- Hinweise auf eine mögliche zunehmende Radikalisierung
- Hinweise auf IS-Sympathisanten
- Informationen über eine islamistische Bestrebung im Sinne des § 4 Abs. 1 Nr. 4 und 5 VerfSchG-LSA
- Islamistische Nordkaukasische Szene (2x)
- Konkretisierung von Personenhinweisen

[156] In einem Fall wurde angegeben, dass Informationen gespeichert wurden, ohne jedoch weitere konkrete Angaben zu machen. Daher sind hier nur 14 Angaben zu den gespeicherten Informationen aufgeführt.

- Mutmaßliches Mitglied bzw. Sympathisant der Terrororganisation „Islamischer Staat“ und dazugehörige Personaldaten.
- Urteil gegen einen Ausländer in einem § 129a/b und 89a StGB-Verfahren hatte Rechtskraft erlangt. Die ABH übermittelte das Datum des Haftendes und Zwei-Drittel-Regelung. Die Möglichkeit, zunächst Asyl zu beantragen und ein ordentliches Verfahren zu durchlaufen, steht also einer Abschiebung aus der Haft entgegen.
- Verdachtsfall mit Gewaltbezug, Speicherung der personenbezogenen Daten

Hinsichtlich der Bewertung des Nutzens der gemäß § 18 Abs. 1a BVerfSchG von den Ausländer- an die Landesverfassungsschutzbehörden übermittelten Informationen für die nachrichtendienstliche Arbeit ergibt sich folgendes Bild: In etwas mehr als 14 Prozent der Fälle wurde der Nutzen als hoch eingeschätzt. In mehr als 40 Prozent der Fälle hatten die Informationen einen geringen bzw. sehr geringen Nutzen für die nachrichtendienstliche Arbeit, während in je knapp einem Viertel der Fälle die Bewertung uneinheitlich ausfiel bzw. keine abschließende Bewertung möglich war (zur Begründung der einzelnen Bewertungen siehe Kapitel 9.3.3, S. 176 ff. im Anhang).

Abb. 10: Bewertung des Nutzens der gemäß § 18 Abs. 1a BVerfSchG übermittelten Informationen für die nachrichtendienstliche Arbeit



Vier LfV gaben an, dass keine Informationen gemäß § 18 Abs. 1a BVerfSchG von den Ausländerbehörden im Erhebungszeitraum übermittelt wurden. Darüber wies ein LfV, das im Evaluationszeitraum drei Fälle übermittelt hatte, darauf hin, dass Initiativübermittlungen von Ausländerbehörden gemäß § 18 Abs. 1a BVerfSchG weder in der Eingangssachbearbeitung noch in der dort geführten Amtsdatei gesondert erfasst würden. Insofern sei eine konkrete Aussage zur Anzahl der Initiativübermittlungen oder zu daraus resultierenden Speicherungen nicht möglich. Zudem erhalte das LfV sowohl im Rahmen von Verfahren zur Personenüberprüfung als auch im Rahmen der Beteiligung an der Sicherheitskonferenz Informationen aus den Ausländerbehörden.

Zusammenfassend lässt sich festhalten, dass die Nutzungsintensität der Regelung auf Bundesländerebene – möglicherweise bedingt durch unterschiedliche Aufgabenprofile – deutlich hinter der auf Bundesebene zurückbleibt. Spontanübermittlungen gemäß § 18 Abs. 1a BVerfSchG erfolgten auf Länderebene eher im Einzelfall. Ein ähnliches Bild zeigt sich beim

Speicherverhalten. Auch hier werden von den Ausländerbehörden übermittelte Informationen in vergleichsweise wenigen Fällen durch die Landesverfassungsschutzbehörden gespeichert.

4.6.3. Rechtswissenschaftliche Bewertung

Mit der Übermittlung nach § 18 Abs. 1a BVerfSchG sind Eingriffe in das allgemeine Persönlichkeitsrecht verbunden.[157] Die Spontanübermittlung stellt sich auf Grundlage der dargestellten Nutzenbewertung als geeignetes Instrument zur Erfüllung nachrichtendienstlicher Aufgaben dar. Gleich geeignete Alternativen sind für die Gewinnung der in Rede stehenden Informationen nicht ersichtlich, insbesondere können die Nachrichtendienste diese nicht selbst erheben, da sie keine Anhörungen durchführen.

Fraglich ist jedoch, ob das Instrument in der sich darstellenden Praxis angemessen ist. Der Eingriff stellt sich im Einzelfall als nicht unerheblich dar, da Informationen zur politischen, religiösen Anschauung, Verhaltensweisen, familiären Beziehungen etc. erhoben werden. Der Eingriff kann allerdings durch die hohen Schutzgüter nachrichtendienstlicher Tätigkeit aufgewogen werden, wie es auch prima facie im Tatbestand angelegt ist. Danach muss der Anhörer tatsächliche Anhaltspunkte für sicherheitsrelevante Informationen feststellen. Dies stellt einen Filter dar, der jedenfalls auch grundrechtsschützend wirken soll, sodass die Nachrichtendienste nicht flächendeckend Informationen aus Asylverfahren erhalten.

Das BAMF ist durch die hohen Asylbewerberzahlen im Erhebungszeitraum nach Aussage der beteiligten Stellen beim BfV nicht in der Lage gewesen, die Ausleitung der Informationen hinreichend zu prüfen. Übergangsweise mag dies mit einer Behördenüberforderung zu erklären sein. Insoweit bleibt abzuwarten, wie sich die vorgenommenen Anpassungen, etwa der (überarbeitete) Kriterienkatalog, auswirken werden. Allerdings bleibt die konstruktive Herausforderung, dass Mitarbeiter des BAMF über die Relevanz der Informationen für die Nachrichtendienste entscheiden müssen. Um einer effektiven Filterfunktion verfahrensmäßig Rechnung zu tragen, müsste eine entsprechend geschulte zentrale Stelle (wie sie prinzipiell beim BAMF existiert) diese Aufgabe übernehmen. Derzeit versucht das BfV die fehlende Ausgangsprüfung beim BAMF durch eine eigene, aufwendige Vorprüfung zu kompensieren. Das BfV betont, dass trotz der hohen Übermittlungs- und Speicherquoten[158] die gesetzlichen Voraussetzungen in jedem Fall umfassend geprüft werden und diese aus der geänderten Sicherheitslage resultieren würden. Die nachrichtendienstliche Eingangskontrolle ist insoweit weiterhin notwendig, aber als Gegenstück einer vorgelagerten Kontrolle bei den datenerhebenden Behörden.

Schließlich bedarf es auch einer Reflexion der Praxis, dass die Anhörerinnen und Anhörer gezielt sicherheitsrelevante Nachfragen stellen, da das Gesetz insoweit eher eine passivische Tendenz zeigt („bekannt gewordene Informationen“).

Eine verfassungsrechtliche Bewertung der Übermittlung personenbezogener Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen ist nur eingeschränkt möglich, da hierzu keine umfassenden Daten vorliegen. Allein Abteilung 6 des BfV hat solche Daten übermittelt in einem Umfang von „deutlich unter einem Prozent“. Dies indiziert, dass jedenfalls keine quasi-automatisierte Weiterleitung stattfindet, sondern – wie § 19 Abs. 3 BVerfSchG vorsieht – eine einzelfallbezogene Entscheidung getroffen wird.

---

[157] Ein Eingriff in das Grundrecht auf Asyl ist nicht gegeben. Denn die Rechtsposition im Asylverfahren wird durch die Sammlung, Verarbeitung und Weiterleitung von sicherheitsrelevanten Informationen weder unmittelbar noch mittelbar-faktisch beeinträchtigt. Insbesondere die Bewertung der asylrelevanten Tatsachen erfolgt ausschließlich durch das BAMF.

[158] Abteilungsübergreifend wurden 78,0 % der übermittelten Informationen gespeichert, s. o.

In Anbetracht dessen, dass Übermittlungen durch die Ausländerbehörden der Länder an die LfV deutlich zurückhaltender als Übermittlungen des BAMF an das BfV erfolgten, besteht kein Anlass zu verfassungsrechtlichen Zweifeln an der empirisch erfassten Übermittlungspraxis.

4.7. § 19 Abs. 4 und 5 BVerfSchG, § 11 Abs. 1 S. 1 MADG

4.7.1. Genese der Regelungen

§ 19 Abs. 4 S. 1-4 BVerfSchG wurde im Zuge der Novellierung des BVerfSchG im Jahre 1990 eingeführt.[159] Eine Ergänzung des Satzes 1 erfolgte mit dem TBG 2002.[160] Damit sollte sichergestellt werden, dass personenbezogene Daten auch zur Gewährleistung der Sicherheit von lebens- und verteidigungswichtigen Einrichtungen im Sinne von § 1 Abs. 4 SÜG übermittelt werden dürfen.[161] Gemäß dem Evaluationsauftrag werden nur diejenigen Bestandteile des § 19 Abs. 4 BVerfSchG miteinbezogen, die für die Evaluierung von § 19 Abs. 5 BVerfSchG relevant sind.

Im Wolff-Gutachten wurde § 19 Abs. 5 S. 1 BVerfSchG kritisiert, sei doch die Vorschrift nicht auf die Fälle der Datenweitergabe an V-Leute begrenzt. Es sei zudem nicht einleuchtend, weshalb der strenge Zweckbindungsgrundsatz nicht auch für Dritte gelten solle. Empfehlenswert sei daher eine Klarstellung.[162] Der Gesetzgeber hat sich bemüht, dieser Kritik im Jahre 2011 Rechnung zu tragen. Durch das Änderungsgesetz wurde die Ausnahmeregelung in Abs. 5 S. 1 konkretisiert.[163] Sie betrifft seitdem Daten, „die an Stellen übermittelt werden, von denen die Daten erhoben werden oder die daran mitwirken." Durch das Änderungsgesetz 2011 wurde darüber hinaus klargestellt, dass in den Fällen, in denen das BfV nach § 8 Abs. 1 S. 2 BVerfSchG um die Übermittlung von Daten ersucht, die übermittelten personenbezogenen Daten Bestandteil der Anfrage sind und somit von den in § 19 Abs. 4 S. 1-4 und 7 BVerfSchG aufgestellten Anforderungen befreit sind. Hingegen regelt § 19 Abs. 5 S. 2 BVerfSchG, dass für diese Anfragen, sofern sie nicht unter die in § 8 Abs. 2 BVerfSchG bezeichneten Mittel fallen, also keine Gegenstände und Mittel zur heimlichen Informationsbeschaffung sind, § 19 Abs. 4 S. 5 und 6 BVerfSchG weiterhin Anwendung findet. Damit dürfen in diesen Fällen die Empfänger der Anfrage, die ihnen übermittelten Daten nur zur Erteilung der Auskunft, jedoch nicht für weitere Zwecke verwenden. Zudem ist der Empfänger sowohl auf die Verwendungsbeschränkung als auch darauf hinzuweisen, dass das BfV den Nachweis der Einhaltung dieser Beschränkung verlangen darf.

§ 11 Abs. 1 S. 1 MADG wurde im Zuge der TBG-Reform 2002 neu gefasst.[164] Das BAMAD erhielt dadurch die Befugnis, gemäß § 19 BVerfSchG Daten an andere Stellen zu übermitteln. Dadurch solle ein Gleichlauf mit den Befugnissen des BfV erreicht werden. Da auch Private Aufgaben der Verteidigung übernehmen könnten, sei die Übermittlung an diese „anderen Stellen" zwingend erforderlich.[165]

Der Verweis auf § 19 Abs. 2-5 BVerfSchG im BNDG wurde jüngst in § 24 Abs. 2 BNDG verschoben.[166]

---

[159] Art. 2 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990, BGBl I Nr. 73 vom 29.12.1990, S. 2975.
[160] Art. 1 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 363, in Kraft getreten am 01.01.2002.
[161] Vgl. Bundestag, Innenausschuss, Bericht, BT-Drs. 14/7864, S. 5.
[162] Vgl. Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011, S. 105.
[163] Art. 1 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2578, in Kraft getreten am 10.01.2012.
[164] Art. 2 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 364, in Kraft getreten am 01.01.2002.
[165] Vgl. Bundesregierung, BT-Drs. 14/7386 (neu), S. 42.
[166] Siehe hierzu ausführlich Kapitel 4.10, S. 88 f.

4.7.2. Empirische Ergebnisse

Hinsichtlich der Übermittlung personenbezogener Daten zur Gewährleistung der Sicherheit von lebens- und verteidigungswichtigen Einrichtungen nach § 1 Abs. 4 SÜG verwies das BfV darauf, dass es sich um absolute Einzelfälle handele. Im Erhebungszeitraum sei es zu keiner Übermittlung gemäß § 19 Abs. 4 BVerfSchG gekommen. Dennoch ist das BfV der Auffassung, dass die Regelung beibehalten werden sollte, da es immer zu Fällen, die durch die Vorschrift erfasst werden, kommen könne. Moniert wurde in Bezug auf § 19 Abs. 4 BVerfSchG die Pflicht, dass dem Betroffenen die Datenübermittlung mitgeteilt werden müsse. Dies würde in der Regel die Aufgabenerfüllung gefährden. Folglich müsse für jeden dieser Fälle eine abschlägige Entscheidung getroffen werden. Nach interner Vorschriftenlage müsse die Nichtmitteilung spätestens alle fünf Jahre überprüft werden. Die Mitteilungspflicht verhindere darüber hinaus, dass Akten vernichtet werden können. Stattdessen müssten sie gesperrt werden. Dies führe insgesamt zu einem unverhältnismäßigen Arbeitsaufwand, da die Rechte des Betroffenen aus Sicht des BfV durch das Antragsverfahren (Übermittlung nur nach Zustimmung des BMI) gesichert seien und Mitteilungspflichten eigentlich sonst nur bei schweren Eingriffen vorgesehen seien (vgl. § 9 Abs. 3 BVerfSchG). Nach Einschätzung des BfV würden somit eigentlich mögliche Übermittlungen durch die Mitteilungspflicht verhindert.
Die Anwendung von § 19 Abs. 5 BVerfSchG gehöre zur täglichen Arbeit des BfV, da es bei der Sammlung von Informationen notwendig ist, beispielsweise einer anderen Stelle (z. B. Hotel/Mietwagenfirma) den Namen der Zielperson zu nennen, um weiterführende Informationen zu erhalten. In solchen Fällen werde der Angesprochene immer aufgefordert, über das Aufklärungsinteresse des BfV Stillschweigen zu wahren. Allerdings werde der ausdrücklich verlangte Vorbehalt, sich über die Verwendung der übermittelten personenbezogenen Daten zu erkundigen, vom BfV als eher kontraproduktiv erachtet. Insgesamt ist das BfV der Auffassung, dass § 19 Abs. 5 BVerfSchG für die tägliche Arbeit unverzichtbar sei und daher beibehalten werden sollte.
Da sowohl § 11 Abs. 1 S. 1 MADG als auch § 24 Abs. 2 BNDG (n. F.) auf § 19 Abs. 2 bis 5 BVerfSchG verweisen, gelten die Änderungen auch für den MAD und den BND. Das BAMAD gab an, dass es sich bei der Übermittlung von Informationen an Private um einen Sonderfall handele. Dies sei auch an der sehr hohen Hürde für solche Übermittlungen erkennbar. Bisher habe es so einen Fall auch noch nicht beim BAMAD gegeben. Grundsätzlich wäre es schon denkbar, dass von dieser Möglichkeit Gebrauch gemacht werde (z. B. wenn Informationen zu einem kurz bevorstehenden Angriff auf einen Flughafen oder ein AKW vorlägen). § 11 Abs. 1 S. 1 i. V. m. § 19 Abs. 5 BVerfSchG komme zur Anwendung, wenn personenbezogene Daten durch das BAMAD über eine Person bei z. B. Nachbarn, Freunden oder ehemaligen Arbeitgebern darüber gesammelt würden, ob bei der betreffenden Person gewisse Auffälligkeiten festgestellt worden wären bzw. welche Bücher gelesen würden oder welche Musik gehört werde. Das BAMAD wies in diesem Zusammenhang jedoch darauf hin, dass in der Praxis nur der Hinweis gegeben werde, die übermittelten Daten nicht für andere Zwecke zu verwenden. In der Praxis werde hingegen regelmäßig nicht nachgefragt, wie der Empfänger der Anfrage mit den Daten umgegangen ist. Zudem würden bei einem möglichen Verstoß keine Sanktionierungsmöglichkeiten bestehen. Daher könne dieser Teil aus Sicht des BAMAD gestrichen werden. Insgesamt sollten die beiden Regelungen aber beibehalten werden.

4.7.3. Rechtswissenschaftliche Bewertung

Die empirische Auswertung der nachrichtendienstlichen Praxis hat keine Hinweise darauf ergeben, dass die in den evaluierten Regelungen statuierten Ausnahmen zur Sicherung der

Wirksamkeit nachrichtendienstlicher Maßnahmen in die verfassungsrechtlichen Grenzen verletzender Weise angewandt worden sind.

4.8. § 10 Abs. 1 und 3 MADG

4.8.1. Genese der Regelung

§ 10 MADG regelt die Übermittlung von Informationen an das BAMAD. § 10 Abs. 1 und Abs. 3 MADG bestanden bereits vor dem Jahre 2002. Das TBG ermöglicht die Übermittlung der Informationen nach Absatz 1 auch für die in § 1 Abs. 1 S. 2 MADG genannten Schutzgüter.[167] Mit dem TBEG wurde die amtliche Registereinsicht des vorherigen § 10 Abs. 4 MADG in dem neuen § 10 Abs. 3 MADG geregelt und auf die in § 1 Abs. 1 S. 2 MADG genannten Schutzgüter erstreckt. An die Stelle der Zustimmung des „Amtschefs des Amtes für den Militärischen Abschirmdienst“ trat die Zustimmung des „Behördenleiters“. Die geänderte Bezeichnung soll dem Umstand Rechnung tragen, dass nicht nur ein Soldat, sondern auch ein Zivilist die Behörde leiten kann.[168] Die Vorschrift ist seitdem nicht mehr verändert worden. Der Evaluationsauftrag erstreckt sich nur auf den Verweis in § 1 Abs. 1 S. 2 MADG (Übermittlung von Informationen an das BAMAD und Einsichtnahme in amtliche Register im Zusammenhang mit Bestrebungen gegen den Gedanken der Völkerverständigung).

4.8.2. Empirische Ergebnisse

Im Erhebungszeitraum gab es keine Fälle, in denen Daten an das BAMAD übermittelt wurden, die einen Bezug zu den in § 1 Abs. 1 S. 2 MADG genannten Schutzgütern hatten. Nach Angabe des BAMAD handele es sich um einen sehr begrenzten Anwendungsbereich. Allerdings könnte es Fälle geben, in denen z. B. ein Finanzamt oder das Bundesamt für zentrale Dienste und offene Vermögensfragen Daten an das BAMAD übermittelt. Jedoch wurde darauf verwiesen, dass andere Übermittlungsvorschriften eine größere Relevanz für das BAMAD besäßen. Es handelt sich lediglich um eine Folgeänderung aufgrund des neu eingefügten § 1 Abs. 1 S. 2 MADG.
Im Erhebungszeitraum gab es ebenfalls keine Fälle, in denen das BAMAD gemäß § 10 Abs. 3 MADG Einsicht in Register zur Wahrnehmung der Aufgaben gemäß § 1 Abs. 1 S. 2 MADG genommen hat. Auch hier handele es sich um einen begrenzten Anwendungsbereich. Allerdings ermögliche die Registereinsicht eine schnelle Gewinnung wichtiger Informationen (z. B. Ausländerzentralregister, Bundeszentralregister, Verkehrszentralregister, Handelsregister). Das BAMAD wies jedoch auf das Problem hin, dass es insbesondere bei kleinen Ämtern, die ein Register führen, für Aufsehen sorge, wenn BAMAD-Mitarbeiterinnen und Mitarbeiter Einsicht in ein Register nehmen wollten. Es habe schon Fälle in der Vergangenheit gegeben, in denen von der Nutzung dieser Möglichkeit abgesehen wurde, da der Aufwand (Fahrt zum jeweiligen Sitz des Registers) zu groß gewesen sei oder keine zu große Aufmerksamkeit auf das Verfahren gelenkt werden sollte. Daher wäre es aus Sicht des BAMAD wünschenswert, wenn der Nachrichtendienst – wie auch das BfV, das BKA oder die LKÄ – einen direkten Zugriff auf die jeweiligen Register bekommen könnten.

4.8.3. Rechtswissenschaftliche Bewertung

Mangels dokumentierter Fälle ist eine verfassungsrechtliche Bewertung der Anwendungspraxis nicht möglich.

---

[167] Art. 2 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 361, in Kraft getreten am 01.01.2002.
[168] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 19.

4.9. § 11 Abs. 1 S. 3 MADG

4.9.1. Genese der Regelung

§ 11 MADG hat die Übermittlung personenbezogener Daten durch das BAMAD zum Gegenstand. Für die vom BfV nach § 18 Abs. 1a S. 1 BVerfSchG (sog. Spontanübermittlungen) übermittelten personenbezogenen Daten verwies die Vorschrift ursprünglich lediglich auf § 18 Abs. 1a S. 2 BVerfSchG.[169] Das TBEG erweiterte den Verweis auf 18 Abs. 1a S. 2-4 BVerfSchG. Es handelt sich um eine Folgeänderung zur Anpassung an § 18 Abs. 1a BVerfSchG.[170]

4.9.2. Empirische Ergebnisse

Im Erhebungszeitraum gab es nur einen Fall, in dem personenbezogene Daten gemäß § 18 Abs. 1a BVerfSchG vom BfV an das BAMAD übermittelt wurden. Die übermittelten Daten, bei denen es sich um das Foto einer Person sowie das Anhörungsprotokoll aus ihrem Asylverfahren handelte, das Hinweise auf seine Zugehörigkeit zu den Taliban enthielt, wurden vom BAMAD gespeichert. Die übermittelten Informationen wurden als teilweise nützlich für die nachrichtendienstliche Arbeit eingestuft, da sie wertige Hintergrunderkenntnisse zum Modus Operandi der regierungsfeindlichen Kräfte in Afghanistan lieferten. Es erfolgte keine Weitergabe der personenbezogenen Daten gemäß § 11 Abs. 1 S. 3 i. V. m. § 18 Abs. 1a BVerfSchG an ausländische öffentliche Stellen bzw. an über- und zwischenstaatliche Stellen.
Im Kontext der Evaluation fiel dem BAMAD auf, dass es mehr Fälle im Erhebungszeitraum gegeben habe, die vom BfV hätten übermittelt werden müssen. So seien in mehreren Fällen Informationen auf Grundlage vom § 10 Abs. 1 MADG vom BAMF übermittelt worden, die jedoch aufgrund des nicht erkennbaren Gewaltbezugs nicht genutzt werden konnten. Dabei sei aufgefallen, dass diese Fälle vom BfV hätten weitergeleitet werden müssen. Dies sei jedoch nicht geschehen. In diesem Zusammenhang betonte das BAMAD, dass die vom BAMF stammenden Informationen sehr wichtig für seine Arbeit seien, da es sich z. B. um Informationen handele, die dem Schutz der Truppe (z. B. Innentäterbedrohung durch afghanische Soldaten) diene oder zur Überprüfung von Ortskräften genutzt werden könnten. Aus diesem Grund sei es wichtig, dass das BAMAD diese Informationen schnell erhalte.
Grundsätzlich könne es vorkommen, dass die vom BAMF übermittelten Informationen an Polizeibehörden, die Staatsanwaltschaft sowie ausländische Nachrichtendienste weitergeleitet würden. Insbesondere bei Übermittlungen an ausländische Nachrichtendienste werde sehr genau geprüft, welches Datenschutzniveau in den jeweiligen Ländern herrsche.
Aus Sicht des BAMAD wäre es wünschenswert, wenn der Nachrichtendienst – analog zu § 18 Abs. 1a BVerfSchG, ggf. durch Ergänzung oder Änderung von § 10 Abs. 1 bzw. § 14 Abs. 6 S. 1 MADG – ebenfalls direkter Empfänger der BAMF-Spontanübermittlungen werden würde.

4.9.3 Rechtswissenschaftliche Bewertung

Für die verfassungsrechtliche Bewertung wird auf die Ausführungen zu § 18 Abs. 1a BVerfSchG verwiesen, soweit sie die grundsätzliche Verfassungsmäßigkeit des Instruments zum Gegenstand haben (siehe Kapitel 4.6.3., S. 83 ff.). Die Anwendungspraxis stellt sich bei § 11 Abs. 1 S. 3 MADG als evident verfassungsrechtlich unbedenklich dar.

---

[169] Art. 1 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 4, in Kraft getreten am 11.01.2007.
[170] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 19.

4.10. § 24 Abs. 1 und 2 BNDG

4.10.1. Genese der Regelung

§ 9 Abs. 1 und 2 BNDG bestanden bereits vor dem Jahre 2002. Mit dem TBG wurde zur Anpassung an den neuen § 18 Abs. 1a BVerfSchG in Abs. 2 ein neuer Satz 2 eingefügt.[171] Das TBEG 2007 nahm Änderungen der Vorschrift vor.[172] Die Übermittlung des BND in § 9 Abs. 1 BNDG ist nicht mehr nur an inländische Behörden möglich, sondern darüber hinaus an alle inländischen öffentlichen Stellen. Im Übrigen erfolgten nur formelle Änderungen zur Anpassung an die sonstigen Bestimmungen des BVerfSchG[173]: Für die Übermittlung von Informationen an andere Stellen verwies § 9 Abs. 2 BNDG neben dem § 19 Abs. 2-4 BVerfSchG auch auf den neu eingefügten § 19 Abs. 5 BVerfSchG. Die Zustimmung zur Übermittlung erfolgt nicht mehr konkret durch den „Chef des Bundeskanzleramtes", sondern durch das „Bundeskanzleramt". Der Verweis auf § 18 Abs. 1a S. 2 wurde erweitert auf § 18 Abs. 1a S. 2-4 BVerfSchG. Seit Ende 2017 finden sich die Regelungen unverändert in § 24 Abs. 1 und 2 BDNG.[174]

4.10.2. Empirische Ergebnisse

Die Änderung des § 9 Abs. 1 BNDG a. F. habe im Erhebungszeitraum keine Bedeutung für den BND gehabt. Allerdings würden keine Statistiken geführt, wie viele Informationen an welche inländischen öffentlichen Stellen übermittelt worden seien. Sehr häufig würden Daten übermittelt, die teilweise aus öffentlichen und teilweise aus nachrichtendienstlich gewonnenem Material bestehen würden. Bei der Weiterleitung von Daten gemäß § 24 Abs.1 BNDG handele es sich um einen üblichen Vorgang. Empfänger der Daten seien beispielsweise Polizeien, Staatsanwaltschaften, LfV, BfV oder Ministerien.
Die Änderung könnte nach Ansicht des BND aber Auswirkungen haben, wenn es öffentliche Stellen gebe, die keine Behörden sind (z. B. die GIZ). Dadurch könnte die Übermittlung erleichtert werden.
Die Empfänger von Übermittlungen gemäß § 24 Abs. 2 S. 1 BNDG i. V. m. § 19 Abs. 4 BVerfSchG seien vor allem Unternehmen, wenn es z. B. um Wirtschaftsschutz gehe. Die Änderung, dass statt des „Chef des Bundeskanzleramtes" „das Bundeskanzleramt" einer Übermittelung gemäß § 19 Abs. 4 BVerfSchG zustimmen müsse, habe keine Auswirkungen auf die Vorbereitung der Entscheidung.
Bei der Übermittlung von Daten gemäß § 24 Abs. 2 S. 1 i. V. m. § 19 Abs. 5 BVerfSchG werde immer auch der gesetzliche Verwendungshinweis gegeben. Die Unternehmen hätten jedoch auch ein Eigeninteresse an einem guten zweckgerichteten Umgang mit den Daten. Dies werde auch durch die Einbeziehung des jeweiligen Sicherheitsbeauftragten eines Unternehmens sichergestellt. Es gebe bislang keine Erkenntnisse über einen möglichen Missbrauch übermittelter Daten. Eine Mitteilung über die Übermittlung personenbezogener Daten an Betroffene erfolge in der Regel nicht. Der BND begründete dies damit, dass normalerweise nur Sachinformationen ohne Personenbezug weitergegeben würden (z. B. Flugrouten von Drogenkurieren an eine Fluglinie) sowie dass in vielen Fällen operative Gründe und/oder Quellenschutz-Aspekte einer Weitergabe personenbezogener Daten entgegenstehen würden.

---

[171] Art. 3 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 364, in Kraft getreten am 01.01.2002.
[172] Art. 4 TBEG vom 05.01.2007, BGBl I Nr. 1 vom 10.01.2007, S. 5, in Kraft getreten am 11.01.2007.
[173] Vgl. Bundesregierung, BT-Drs. 16/2921, S. 19.
[174] Art. 1 Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23.12.2016, BGBl I Nr. 67 vom 30.12.2016, S. 3346.

Informationsübermittlungen gemäß § 24 Abs. 2 S. 2 BNDG i. V. m. § 18 Abs. 1a BVerfSchG habe es bisher nicht gegeben.

4.10.3. Rechtswissenschaftliche Bewertung

Mangels dokumentierter Fälle ist eine verfassungsrechtliche Bewertung der Anwendungspraxis nicht möglich. Im Übrigen wird für die verfassungsrechtliche Bewertung auf die Ausführungen zu § 18 Abs. 1a BVerfSchG verwiesen, soweit diese das Instrument der Spontanübermittlung als solcher betreffen (siehe Kapitel 4.6.3., S. 83 ff.).

4.11. § 1 Abs. 4 und 5 SÜG

4.11.1. Genese der Regelung

Der Evaluationsauftrag erstreckt sich auf die Änderungen des SÜG durch das TBG, das TBEG, das Änderungsgesetz und das Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen.[175] Zentrale Änderung war die Einführung des vorbeugenden personellen Sabotageschutzes in § 1 Abs. 4 und 5 SÜG im Jahr 2002.[176] Mit dem Änderungsgesetz 2011 wurde ein neuer § 1 Abs. 4 S. 2 SÜG angefügt, der das Ziel des vorbeugenden personellen Sabotageschutzes näher beschreibt und der Klarstellung dienen soll.[177] Die Vorschrift betrifft bewusste Sabotagehandlungen – vornehmlich mit terroristischem Hintergrund. Allgemeine Zulässigkeitsanforderungen für die Tätigkeit an sicherheitsrelevanten Stellen sollen davon nicht erfasst sein. Die Klarstellung hat insbesondere Bedeutung für die Bewertung sicherheitserheblicher Erkenntnisse nach dem neuen § 14 Abs. 3 S. 2 SÜG.[178]
Die Zuständigkeit beim Sabotageschutz wurde in § 3 SÜG und § 25 SÜG geregelt. Ursprünglich regelte § 3 Abs. 1 S. 1 Nr. 5 den Sabotageschutz im öffentlichen Bereich. Durch die umfassende Novellierung im Jahr 2017[179] wurden u. a. die Regeln über die Zuständigkeit in § 3 Abs. 1 SÜG neugefasst. Die Zuständigkeit für den vorbeugenden personellen Sabotageschutz im öffentlichen Bereich ergibt sich nunmehr unmittelbar aus Nummer 1. Nummer 5 enthält jetzt eine Sonderregelung für Bauangelegenheiten des Bundes, die durch Bauverwaltungen der Länder im Wege der Organleihe ausgeführt werden und für die Personen aus nichtöffentlichen Stellen zu überprüfen sind..[180] Für Bauangelegenheiten ziviler Behörden ist die Bundesanstalt für Immobilienaufgaben (BImA), im Geschäftsbereich des BMVg die nutzende Verwaltung zuständig. Die Zuständigkeit für den vorbeugenden personellen Sabotageschutz im nichtöffentlichen Bereich ergibt sich aus § 25 Abs. 2 S. 1 SÜG.
Durch das Satellitendatensicherheitsgesetz (SatDSiG) erfolgte im Jahr 2007 eine Ergänzung des § 3 Abs. 2 S. 1 SÜG (s. § 33 Nr. 2 SatDSiG). Die Verfassungsschutzbehörden wirken danach gemäß § 3 Abs. 2 S. 1 Nr. 2 BVerfSchG mit bei der Sicherheitsüberprüfung von Perso-

---

[175] Art. 5 des Gesetzes zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen.
[176] Art. 5 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 365, in Kraft getreten am 01.01.2002.
[177] Art. 4 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2579, in Kraft getreten am 10.01.2012. Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 14/7386, S. 43; Bundesregierung, BT-Drs. 17/6925, S. 18 f.
[178] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 18 f.
[179] Anlass für die Novellierung war die Implementierung der Grundsätze des materiellen Geheimschutzes sowie die Vereinfachung des Verfahrens der Sicherheitsüberprüfung, RegEntw, BT-Drs.18/11281 S. 39 f.
[180] BT-Drs. 18/11281, S. 55.

nen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen.[181] Die Ergänzung des § 3 Abs. 2 S. 1 SÜG um Nummer 2 des § 3 Abs. 2 S. 1 BVerfSchG ist eine Folgeänderung anlässlich der Einführung des vorbeugenden personellen Sabotageschutzes in das SÜG, die im TBG und auch im TBEG versehentlich unterblieben war.[182]

Das Änderungsgesetz 2011 enthielt Ergänzungen bisheriger Regelungen in § 2 Abs. 2 S. 1, § 12 Abs. 4 S. 3, § 13 Abs. 2a, § 14 Abs. 3 S. 2 und § 32 Abs. 1 S. 1 SÜG, um den Besonderheiten des vorbeugenden personellen Sabotageschutzes Rechnung zu tragen.[183] Zudem genügte für den vorbeugenden personellen Sabotageschutz bis zum Jahre 2011 eine einfache Sicherheitsüberprüfung gemäß § 8 Abs. 1 Nr. 3 SÜG. Diese wurde durch das Erfordernis einer erweiterten Sicherheitsüberprüfung in § 9 Abs. 1 Nr. 3 SÜG ersetzt und eine Übergangsbestimmung in § 38a SÜG geschaffen.[184] Die Erhöhung des Überprüfungsniveaus durch zusätzliche Überprüfungsmaßnahmen (§ 12 Absatz 2 SÜG) sei erforderlich aus Gründen der Sicherheit, zur Anpassung an die entsprechenden Regelungen im Atomgesetz und Luftsicherheitsgesetz (§ 12b AtomG und § 7 LuftSiG, sog. Zuverlässigkeitsüberprüfung) und um zukünftig Mehrfachprüfungen zu vermeiden.[185] Allerdings wurden die Anforderungen an die Sicherheitserklärung leicht reduziert (§ 13 Abs. 2a SÜG). Ferner wurde die Möglichkeit geschaffen, ausnahmsweise eine nicht sicherheitsüberprüfte Person in ständiger Begleitung an einer sicherheitsempfindlichen Stelle zu beschäftigen, sofern sie mit einer unaufschiebbaren sicherheitsempfindlichen Tätigkeit betraut werden soll, für die keine überprüften Personen zur Verfügung stehen (§ 9 Abs. 2 Nr. 1 SÜG); im Übrigen für „in der Regel höchstens einen Tag“ (§ 9 Abs. 2 Nr. 2 SÜG). 2015 wurde dieser Zeitraum auf „höchstens vier Wochen“ erweitert.[186]

Im Zuge der Novellierung 2017 wurde mit Einfügung von § 9 Abs. 3 SÜG geregelt, dass bei Neufeststellung von sicherheitsempfindlichen Stellen die Sicherheitsüberprüfung für eine dort bereits tätige Person unverzüglich durchzuführen ist. Hierdurch wurde verhindert, dass die Arbeit an neu eingestuften sicherheitsempfindlichen Stellen nicht komplett niedergelegt werden muss, bis der dort bereits zuvor tätige Personenkreis erfolgreich die erforderliche Sicherheitsüberprüfung durchlaufen hat. Die bei der SÜ durchzuführenden Maßnahmen der mitwirkenden Behörde wurden dergestalt erweitert, dass nunmehr eine Abfrage beim Zentralen Staatsanwaltschaftlichen Verfahrensregister und beim Ausländerzentralregister erfolgt (§ 12 Abs. 1 Nr. 2 und Nr. 2a) sowie eine Internetrecherche (z. B. bei „sozialen Netzwerken“) möglich ist ,§ 12 Abs. 3a S. 1 und 2 SÜG).

Mit der Novellierung von § 17 SÜG wurde zusätzlich das Sicherheitsniveau erhöht, indem nun Aktualisierungsverfahren mit Maßnahmen nach § 12 Abs. 1 SÜG und Wiederholungsüberprüfungen im Abstand von fünf Jahren alternierend durchzuführen sind.[187] Ferner sind

---

[181] Vgl. § 33 SatDSiG vom 23.11.2007, BGBl I Nr. 58, vom 28.11.2007, S. 2597.

[182] Vgl. Bundesregierung, BT-Drs. 16/4763, S. 31.

[183] Näher dazu Bundesregierung, BT-Drs. 17/6925, S. 19 f. Nach § 13 Abs. 2a SÜG sind für die Sicherheitserklärung einige Angaben nicht erforderlich, weil sich hieraus keine Anhaltspunkte für einen tatsächlichen Sicherheitsgewinn in Bezug auf terroristische Sabotagehandlungen ergeben haben. § 14 Abs. 3 S. 2 SÜG dient der Klarstellung der Bewertung. Nach § 32 Abs. 1 S. 1 SÜG gelten Reisebeschränkungen nicht für den Bereich des vorbeugenden personellen Sabotageschutzes.

[184] Vgl. Art. 4 Änderungsgesetz vom 07.12.2011, BGBl I Nr. 64 vom 13.12.2011, S. 2579, in Kraft getreten am 10.01.2012.

[185] Vgl. Bundesregierung, BT-Drs. 17/6925, S. 19.

[186] Art. 2 G v. 03.12.2015, BGBl I, 2161, m. W. v. 10.12.2015. Zur Begründung vgl. BT-Drs. 18/5924, S. 11.

[187] Dazu RegEntw, BT-Drs.18/11281 S. 82.

Änderungen der persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse sowie sicherheitsrelevante Informationen dem Geheimschutz-/Sabotageschutzbeauftragten durch die Personalstelle ausdrücklich mitzuteilen (§ 15a SÜG), bisher wurde dies aus § 18 Abs. 2 SÜG abgeleitet.[188] Die §§ 24, 25 SÜG – Anwendungsbereich und Zuständigkeit im nichtöffentlichen Bereich – wurden im Wesentlichen redaktionell neugefasst.
Im Jahr 2002 erfolgte eine Änderung des § 1 Abs. 3 S. 2 MADG.[189] Es handelt sich um eine Klarstellung, dass sich die Befugnisse des BAMAD bei der Mitwirkung an Sicherheitsüberprüfungen aus Gründen des vorbeugenden personellen Sabotageschutzes ebenfalls aus dem Sicherheitsüberprüfungsgesetz ergeben.[190]
Die Verordnung zur Feststellung der Behörden des Bundes mit Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wie die der Nachrichtendienste des Bundes und zur Feststellung der öffentlichen Stellen des Bundes und der nichtöffentlichen Stellen mit lebens- oder verteidigungswichtigen Einrichtungen (Sicherheitsüberprüfungsfeststellungsverordnung - SÜFV) wurde im Jahre 2003 erlassen und 2007 neu bekanntgemacht.[191] In ihr wird festgelegt, welche Stellen oder Teile davon lebens- oder verteidigungswichtig sind und welches Bundesministerium für die nichtöffentlichen Stellen zuständig ist. Sie wurde durch die Dritte Verordnung zur Änderung der Sicherheitsüberprüfungsfeststellungsverordnung[192], die am 9. Januar 2016 in Kraft trat, geändert. Danach wurden Unternehmen, die mit dem Aufbau oder Betrieb der Informations- und Kommunikationstechnik des Bundes beauftragt sind, als lebenswichtige Einrichtung definiert (§ 9a Nr. 2 SÜFV). § 10 Abs. 1 Nr. 1 SÜFV wurde insoweit modifiziert, als dass nicht mehr die einzelnen Telekommunikationsdienste, sondern die Transportebene (Übertragungswege) als kritische Telekommunikationsinfrastruktur in den Blick genommen wurde. § 10 Nr. 2 SÜFV a.F. wurde zugunsten bereits bestehender spezialgesetzlicher Vorschriften im Waffen- und Sprengstoffgesetz zur Vermeidung von Doppelüberprüfungen mit den damit verbundenen Inkonsistenzen gestrichen. Nummer 3 wurde in § 10a SÜFV verlagert und die Anwendbarkeit insoweit eingeschränkt, als dass eine Lebenswichtigkeit im Sinne von § 1 Absatz 5 Satz 1 SÜG nicht gegeben ist, wenn der Betrieb ausreichend durch organisatorische oder technische Maßnahmen gegen Eingriffe Unbefugter geschützt und dies im Sicherheitsbericht nach § 9 der Störfall-Verordnung dokumentiert ist.
Mit Artikel 1 des Gesetzes zur Änderung des Soldatengesetzes und weiterer soldatenrechtlicher Vorschriften[193] wurde eine einfache Sicherheitsüberprüfung (Ü1) nach dem SÜG für Soldaten eingeführt (§ 37 Abs. 3 SG[194], sog. Soldateneinstellungsüberprüfung). Wenn Letzteres auch nicht unmittelbar Gegenstand der Evaluation war, so wurde hierauf wegen der weitreichenden Bedeutung in den Interviews Bezug genommen.

4.11.2. Empirische Ergebnisse

Im Folgenden werden die Ergebnisse der von BfV, BMVg und BMWi übermittelten Fallzahlen für den Zeitraum 1. Januar 2015 bis 31. Dezember 2017 – differenziert nach nichtöffentlichem,

---

[188] Vgl. dazu auch RegEntw, BT-Drs.18/11281 S. 81.
[189] Art. 2 TBG vom 09.01.2002, BGBl I Nr. 3 vom 11.01.2002, S. 363.
[190] Vgl. Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 14/7386 (neu), S. 42.
[191] Vgl. SÜFV vom 30.07.2003, BGBl I Nr. 39 vom 08.08.2003, S. 1553, neu bekanntgemacht am 12.09.2007, BGBl I Nr. 48 vom 20.07.2007, S. 2294.
[192] Dritte Verordnung zur Änderung der Sicherheitsüberprüfungsfeststellungsverordnung, BGBl I Nr. 49, S. 2186, in Kraft getreten am 9.1.2016.
[193] BGBl I Nr. 15 vom 30.03.2017, S. 562.
[194] Zuletzt geändert durch Art. 3 des Gesetzes zu bereichsspezifischen Regelungen der Gesichtsverhüllung und zur Änderung weiterer dienstrechtlicher Vorschriften vom 08.06.2017, BGBl I Nr. 36 vom 14.06.2017, S. 1570.

öffentlichem und militärischen (Sicherheits-)Bereich – dargestellt und um die Einschätzungen der Behörden, die von den Regelungen zum vpS betroffen sind, ergänzt.

4.11.2.1. Statistische Ergebnisse und Einschätzungen der betroffenen Behörden

Die Einführung des vorbeugenden personellen Sabotageschutzes in das Sicherheitsüberprüfungsgesetz sollte der entschlossenen, aber auch wirkungsvollen Bekämpfung des internationalen Terrorismus dienen.[195] Durch Sicherheitsüberprüfungen sollte verhindert werden, dass potenzielle Innentäter an sicherheitsempfindlichen Stellen in lebens- und verteidigungswichtige Einrichtungen oder einen militärischen Sicherheitsbereich gelangen und dort Sabotageakte begehen können, die

1. die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden,
2. Gefahren für die öffentliche Sicherheit oder Ordnung entstehen lassen oder
3. die Verteidigungsbereitschaft der Bundeswehr und verbündeter Streitkräfte sowie der Zivilen Verteidigung erheblich gefährden.

Mit der Einfügung von § 1 Abs. 4 S. 2 SÜG im Rahmen des Änderungsgesetzes 2011 wurde diese Zielsetzung, die bereits im TBEG zum Ausdruck kam[196], auf gesetzlicher Ebene noch einmal ausdrücklich unterstrichen. Für Personen, die an sicherheitsempfindlichen Stellen beschäftigt werden sollen, ist vor Aufnahme ihrer sicherheitsempfindlichen Tätigkeit seit dem 10. Januar 2012 eine erweiterte Sicherheitsüberprüfung (Ü2) durchzuführen. Diese sieht neben einer Identitätsprüfung auch die Einbeziehung von Erkenntnissen der Polizeidienststellen der Wohnsitze in der Regel der letzten fünf Jahre der/des Betroffenen, insbesondere im Hinblick auf laufende Ermittlungsverfahren, vor, die verfahrensmäßig über die jeweiligen Landeskriminalämter (LKÄ) gesteuert werden. Eine Einbeziehung des Partners/der Partnerin in die Ü2 im vorbeugenden personellen Sabotageschutz erfolgt hingegen nicht.[197]
Grundsätzlich lassen sich drei Bereiche (1. nichtöffentlicher Bereich, 2. öffentlicher Bereich und 3. militärischer Sicherheitsbereich) unterscheiden, in denen eine solche SÜ durchgeführt wird. In der SÜFV ist sowohl für den öffentlichen Bereich (§§ 2 bis 9 SÜFV) als auch für den nichtöffentlichen Bereich (§§ 9a bis 11 SÜFV) festgelegt, welche lebens- und verteidigungswichtigen Einrichtungen über sicherheitsempfindliche Stellen verfügen. Der militärische Sicherheitsbereich wird bereits in § 1 Abs. 4 S. 1 SÜG hinreichend definiert und findet daher in der SÜFV keine Erwähnung. Bei einer ersten Betrachtung der Zahlen zu den eingeleiteten und abgeschlossenen SÜ fällt auf, dass im militärischen Sicherheitsbereich mit Abstand die meisten SÜ anfallen, während der nichtöffentliche und der öffentliche Bereich deutlich hinter den Zahlen des Geschäftsbereichs des BMVg zurückbleiben. Hinsichtlich der Anwendungspraxis ist festzuhalten, dass einige Unterschiede zwischen den drei Bereichen bestehen. Dementsprechend erfolgt hier eine differenzierte Darstellung.

4.11.2.1.1. Nichtöffentlicher und öffentlicher Bereich

Da die Bewertung des nichtöffentlichen und öffentlichen Bereiches durch das BfV als mitwirkende Stelle insgesamt erfolgt, ist ein gemeinsames Oberkapitel erforderlich.

Nichtöffentlicher Bereich

Die SÜFV definiert, welche Unternehmen als lebens- oder verteidigungswichtige Einrichtungen gemäß § 1 Abs. 5 SÜG anzusehen sind. Von der SÜFV erfasste Einrichtungen haben

[195] So Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 14/7386 (neu), S. 35.
[196] Vgl. Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 14/7386 (neu), S. 43.
[197] § 2 Abs. 2 S. 1 SÜG; Warg, in: Schenke/Graulich/Ruthig, Sicherheitsrecht (2014), § 8 SÜG Rn. 4.

mindestens eine sicherheitsempfindliche Stelle, wobei die Identifikation der sicherheitsempfindlichen Stelle im nichtöffentlichen Bereich durch das jeweilige Unternehmen selbst erfolgt. In einem ersten Schritt erfolgt eine Art Registrierung der Einrichtungen beim zuständigen Fachreferat des BMWi. Dort werden 871 Unternehmen (Stand: Oktober 2017) betreut. Das Referat prüft dann, ob es sich bei den antragstellenden Unternehmen um eine lebenswichtige Einrichtung oder um eine sog. Fremdfirma handelt. Fremdfirmen (z. B. Dienstleister oder Handwerksbetriebe) verfügen über keine eigenen sicherheitsempfindlichen Stellen, entsenden jedoch Personal zum Einsatz an solche Stellen. Das Personal dieser Firmen hat nach Angaben des BMWi einen nicht unerheblichen Anteil an der Gesamtzahl der Überprüfungen.
Bei verteidigungswichtigen Einrichtungen meldet das Unternehmen dem BMVg, welche Bereiche aus seiner Sicht als sicherheitsempfindliche Stellen anzusehen sind. Kommt das BMVg nach eigener Einschätzung zu dem Schluss, dass es sich tatsächlich um eine solche handelt, ersucht es anschließend um das Einvernehmen des BMI. Nach Erteilung des Einvernehmens erhält das Unternehmen vom BMVg eine entsprechende Bestätigung. Das BMWi erhält ebenfalls eine Mitteilung, die als Grundlage für die Durchführung der entsprechenden SÜ (§ 10 Abs. 2 SÜFV) gilt.
In einem zweiten Schritt werden die Personenprüfungen wie folgt durchgeführt: Das Fachreferat prüft die in der Sicherheitserklärung und im Antrag auf SÜ gemachten Angaben und erfasst die Daten, sofern sie vollständig und richtig sind. In vielen Fällen waren die Angaben zur Person fehlerhaft oder unvollständig (Name, Geburtsdatum/-ort, Wohnsitze (In- und Ausland)). Dies führte in der Vergangenheit zu Verzögerungen im Verfahren von drei bis vier Wochen. Aufgrund der noch nicht abgeschlossenen Umsetzung der elektronischen Sicherheitserklärung wurde vom BMWi-Fachreferat selbst ein PDF programmiert, das ein Ausfüllen der Sicherheitserklärung am PC ermöglicht und Prüfroutinen enthält, die ein unvollständiges/ fehlerhaftes Ausfüllen der Sicherheitserklärung verhindern und dadurch zur Reduzierung der Zahl zurückgesendeter Sicherheitserklärung beitragen soll.
Das Original der Sicherheitserklärung wird dann vom Fachreferat an das BfV geschickt, das als mitwirkende Behörde die Maßnahmen der erweiterten SÜ nach § 12 Abs. 1 bis 2 und 3a SÜG durchführt. Hierzu gehören:

- Sicherheitsmäßige Bewertung der Angaben in der Sicherheitserklärung,
- Abfrage der Erkenntnisse der Verfassungsschutzbehörden Bund/Länder,
- Unbeschränkte Auskunft aus dem Bundeszentralregister,
- Abfrage beim Zentralen Staatsanwaltschaftlichen Verfahrensregister,
- Anfrage an das Bundeskriminalamt (BKA), Bundespolizeipräsidium, BND und BAMAD,
- Anfrage an Polizeidienststellen der innegehabten Wohnsitze in der Regel der letzten fünf Jahre über die LKÄ sowie eine
- Identitätsprüfung.

Soweit im Einzelfall erforderlich, erfolgt bei ausländischen betroffenen Personen, die keine freizügigkeitsberechtigten Unionsbürger sind, ein Ersuchen um eine Übermittlung der nach § 3 Abs. 1 und 2 Nrn. 5, 6 und 9 des AZR-Gesetzes gespeicherten Daten.
Darüber hinaus wurde die Einsichtnahmemöglichkeit in öffentlich sichtbare Internetseiten und in den öffentlich sichtbaren Teil sozialer Netzwerke, in denen die betroffene Person Mitglied ist, geschaffen und die Abfrage bei ausländischen Sicherheitsbehörden im Falle eines Aus-

landsaufenthalts von sechs Monaten und mehr in den letzten fünf Jahren inklusive substituierender Maßnahmen (z. B. die Einholung eines polizeilichen Führungszeugnisses des jeweiligen Landes) gesetzlich geregelt.
Die Durchführung dieser Sicherheitsmaßnahmen dauert im Durchschnitt mindestens drei bis vier Monate. Das BfV führt bei den eingegangenen Unterlagen eine Plausibilitäts- und Vollständigkeitsprüfung durch und startet dann die in § 12 SÜG vorgesehenen Anfragen. Zu unterscheiden sind hier automatisierte Anfragen über NADIS sowie beim Bundeszentralregister, beim BKA und bei der Bundespolizei. Die Abfrage bei den LKÄ erfolge momentan noch mittels einer schriftlichen Anfrage per Post. Teilweise würden die Daten von den LKÄ auch per Post ans BfV übermittelt. Mit einigen LKÄ würden Daten per E-Mail ausgetauscht. In der 19. Legislaturperiode sei jedoch eine automatisierte Abfragemöglichkeit geplant.
Das BfV bewertet die Ergebnisse der durchgeführten Maßnahmen in einem Votum, das dann dem BMWi als Entscheidungsgrundlage zur Verfügung gestellt werde. Bei Überprüfungen ohne Erkenntnisse fällt beim BfV ein Arbeitsaufwand von durchschnittlich insgesamt 45 Minuten[198], bei Überprüfungen mit sicherheitserheblichen Erkenntnissen von durchschnittlich insgesamt 460 Minuten[199] an. Das BMWi bewertet wiederum das Votum des BfV und entscheide unter Berücksichtigung des jeweiligen Einzelfalls, insbesondere im Hinblick auf die vorgesehene Tätigkeit des Betroffenen, ob dieser an einer sicherheitsempfindlichen Stelle eingesetzt werden kann. Es ist bei seiner Entscheidung nicht an das Votum des BfV gebunden.
Gelangt das Fachreferat zu der Auffassung, dass beim Betroffenen ein Sicherheitsrisiko vorliegen könnte, wird der betroffenen Person die Gelegenheit gegeben, sich persönlich zu den für die Entscheidung erheblichen Tatsachen zu äußern. Gelingt es der betroffenen Person, die sicherheitserheblichen Erkenntnisse auszuräumen, wird die neue Sachlage zwischen BMWi und BfV erörtert und im Anschluss daran die ggf. positive Entscheidung dem Unternehmen mitgeteilt.
Für den Fall, dass keine neuen, die betroffene Person entlastenden Informationen im Rahmen der Anhörung gewonnen werden konnten, wird den Unternehmen die negative Entscheidung (ohne Angabe von Gründen) mitgeteilt. Das Ergebnis der SÜ sowie die erforderlichen Angaben zum Abschluss der Überprüfung werden in einer Datenbank erfasst. Vor der gesetzlichen Änderung im Jahr 2011 wurden unterschiedliche Kriterien bei der Bewertung zu Grunde gelegt. Während das BMWi das Instrument unter der Prämisse „Bekämpfung des internationalen Terrorismus“[200] verstand und die Entscheidungen in Bezug auf potenzielle Saboteure als Innentäter[201] traf, nahm das BfV stärker eine allgemeine Zuverlässigkeit in den Blick. Die Gesetzesänderung führte dann zu einer Veränderung der letztgenannten Bewertungspraxis, sodass sich die Zahl der festgestellten Sicherheitsrisiken deutlich reduzierte.
Im nichtöffentlichen Bereich können folgende Ergebnisarten bei der Durchführung von SÜ im vorbeugenden personellen Sabotageschutz unterschieden werden:

1. *Ohne Erkenntnisse:*

   Es gibt keine Anhaltspunkte für ein Sicherheitsrisiko.

2. *Sicherheitserhebliche Erkenntnisse:*

   Eine Erkenntnis ist dann sicherheitserheblich, wenn sich aus ihr ein Anhaltspunkt für ein Sicherheitsrisiko ergibt (§ 5 Abs. 2 SÜG). Aus § 14 Abs. 1 S. 2 SÜG sowie der nach § 14

[198] 40 Minuten (mittlerer Dienst) und 5 Minuten (gehobener Dienst).
[199] 60 Minuten (mittlerer Dienst) und 400 Minuten (gehobener Dienst).
[200] So Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 14/7386 (neu), S. 35.
[201] So Bundesregierung, BT-Drs. 17/6925, S. 18 f.

Abs. 3 S. 2 SÜG erforderlichen Bewertung kann resultieren, dass eine Erkenntnis zwar weiter sicherheitserheblich ist, aber nicht zur Feststellung eines Sicherheitsrisikos führt.

3. *Sicherheitsrisiko:*

   Ein Sicherheitsrisiko wird dann festgestellt, wenn sich im Rahmen einer an § 1 Abs. 4 S. 2 SÜG orientierten Gesamtwürdigung des Einzelfalls insbesondere im Hinblick auf die vorgesehene Tätigkeit des Betroffenen tatsächliche Anhaltspunkte erhärten, die

   - Zweifel an der gebotenen Zuverlässigkeit bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit begründen,
   - eine besondere Gefährdung, insbesondere die Besorgnis einer Erpressbarkeit, bei möglichen Anbahnungs-/Werbungsversuchen ausländischer Nachrichtendienste, krimineller oder terroristischer Vereinigungen oder extremistischer Organisationen, die Bestrebungen im Sinne von § 3 Abs. 1 BVerfSchG verfolgen, begründen oder
   - Zweifel am Bekenntnis zur freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes oder jederzeitigen Eintreten für deren Erhaltung begründen.

Zwischen Januar 2015 und Dezember 2017 wurden im nichtöffentlichen Bereich insgesamt 14.736 SÜ eingeleitet, während 14.272 SÜ zum Abschluss gebracht werden konnten. In 95 Prozent der Fälle wurden hierbei keine Probleme festgestellt. In knapp fünf Prozent der Fälle gab es sicherheitserhebliche Erkenntnisse anderer Art. In lediglich einem Fall wurde ein Sicherheitsrisiko festgestellt.

Tab. 17: SÜ im nichtöffentlichen Bereich 2015-2017

Nichtöffentlicher Bereich	**2015**	**2016**	**2017**	**Gesamt**
Eingeleitete SÜ	5.544	4.185	5.007	14.736
Abgeschlossene SÜ, davon	5.296	4.458	4.518	14.272
Ohne Erkenntnisse	*5.027*	*4.224*	*4.338*	*13.589*
Sicherheitserhebliche Erkenntnisse anderer Art, davon:	*269*	*234*	*180*	*683*
Sicherheitsrisiko	*-*	*-*	*1*	*1*

Auffällig ist, dass sich die Zahl der im Zeitraum 2015 bis 2017 eingeleiteten sowie abgeschlossenen SÜ gegenüber dem Zeitraum 2012 bis 2014 um knapp 36 Prozent bzw. mehr als 33 Prozent deutlich verringert hat.
Im Rahmen der SÜG-Novelle wurde darüber hinaus festgelegt, dass für Sicherheitsüberprüfungen nach dem SÜG nach der Erstüberprüfung alle fünf Jahre abwechselnd eine Aktualisierung und Wiederholungsprüfung erfolgen soll. Bei der *Aktualisierung* wird die vorhandene Sicherheitserklärung handschriftlich ergänzt, sofern es Änderungen gegeben hat. Zudem werden nur die Maßnahmen nach § 12 Abs. 1 SÜG im erforderlichen Umfang durchgeführt (siehe auch § 28 Abs. 2 SÜG). Bei der *Wiederholungsprüfung* füllt die betroffene Person eine neue Sicherheitserklärung aus. In diesem Fall werden die Maßnahmen gemäß § 12 SÜG in vollem Umfang durchgeführt (siehe auch § 17 Abs. 2 S. 3 SÜG). Im Zuge des Art. 2 des Gesetzes zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen wurde § 9 Abs. 2 Nr. 2 SÜG dahin gehend geändert, dass die Ausnahmeregelung,

nicht sicherheitsüberprüftes Personal kurzzeitig unter ständiger Begleitung an einer sicherheitsempfindlichen Stelle beschäftigen zu können, von „in der Regel höchstens einen Tag“ auf „höchstens vier Wochen“ ausgedehnt wurde.

Öffentlicher Bereich

Im *öffentlichen Bereich* ist das Verfahren weitgehend mit dem im nichtöffentlichen Bereich identisch. Auch hier ist das BfV als mitwirkende Behörde für die Durchführung der Überprüfungsmaßnahmen zuständig. Einziger Unterschied ist, dass die Sabotageschutzbeauftragten der Behörden, in denen eine Person an einer sicherheitsempfindlichen Stelle eingesetzt werden soll, als zuständige Stelle letztlich auch die Entscheidung darüber treffen, ob die Tätigkeit aufgenommen werden kann oder nicht. Eine Ausnahme im Vergleich zum nichtöffentlichen Bereich stellt die Bundesbank dar. Auf Grundlage eines BMI-Erlasses existiert hier eine Sonderreglung hinsichtlich der SÜ im vorbeugenden personellen Sabotageschutz. Dieser stellt nicht nur auf terroristische Gefahren ab, sondern auch auf sonstige Gefährdungen, die sich spezifisch im Hinblick auf die vorgesehene Tätigkeit ergeben (etwa Untreue i. S. d. § 266 StGB).
Im Geschäftsbereich des BMI dauert die Überprüfung einer betroffenen Person durch das BfV in der Regel zehn Wochen. Für einen Fall ohne sicherheitserhebliche Erkenntnisse benötigen der Geheimschutz-/Sabotageschutzbeauftragte und dessen Mitarbeiterinnen und Mitarbeiter etwa 45 Minuten Nettoarbeitszeit (10-15 Minuten für die Prüfung der Sicherheitserklärung sowie 30 Minuten für die Belehrung). Bei Fällen mit sicherheitserheblichen Erkenntnissen, bei denen das BfV ein Sicherheitsrisiko sehe, würden noch rund 60 Minuten für die Anhörung hinzukommen. Die Feststellung eines Sicherheitsrisikos führt dazu, dass die betroffene Person nicht an der sicherheitsempfindlichen Stelle eingesetzt werden kann. Unter Umständen müsse die Person dann umgesetzt oder versetzt werden. Bei gravierenden Erkenntnissen würden diese an die Personalstelle zum Zwecke einer etwaigen disziplinarrechtlichen Verfolgung sowie dienst- oder arbeitsrechtlicher Maßnahmen übermittelt, sofern dies zu dem mit der Überprüfung verfolgten Zweck erforderlich sei.
Im öffentlichen Bereich können folgende Ergebnisarten bei der Durchführung von SÜ im vorbeugenden personellen Sabotageschutz unterschieden werden:

1. *Ohne Erkenntnisse:*

   Es gibt keine Anhaltspunkte für ein Sicherheitsrisiko.

2. *Sicherheitserhebliche Erkenntnisse:*

   Eine Erkenntnis ist dann sicherheitserheblich, wenn sich aus ihr ein Anhaltspunkt für ein Sicherheitsrisiko ergibt.

3. *Sicherheitshinweise:*

   Das BfV kann dem Sabotageschutzbeauftragten fallbezogene Sicherheitshinweise geben.

4. *Sicherheitsrisiko:*

   Ein Sicherheitsrisiko wird dann festgestellt, wenn sich im Rahmen einer an § 1 Abs. 4 S. 2 SÜG orientierten Gesamtwürdigung des Einzelfalls insbesondere im Hinblick auf die vorgesehene Tätigkeit des Betroffenen tatsächliche Anhaltspunkte erhärten, die

   - Zweifel an der gebotenen Zuverlässigkeit bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit begründen,

- eine besondere Gefährdung, insbesondere die Besorgnis einer Erpressbarkeit, bei möglichen Anbahnungs-/Werbungsversuchen ausländischer Nachrichtendienste, krimineller oder terroristischer Vereinigungen oder extremistischer Organisationen, die Bestrebungen im Sinne von § 3 Abs. 1 BVerfSchG verfolgen, begründen oder
- Zweifel am Bekenntnis zur freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes oder jederzeitigen Eintreten für deren Erhaltung begründen.

Insgesamt wurden zwischen Januar 2015 und Dezember 2017 10.317 SÜ im öffentlichen Bereich eingeleitet. Im gleichen Zeitraum wurden 10.786 SÜ abgeschlossen. Rund 97 Prozent der SÜ wurden ohne sicherheitserhebliche Erkenntnisse abgeschlossen. In etwa mehr als drei Prozent der Fälle wurden hingegen sicherheitserhebliche Erkenntnisse gewonnen, wobei in sechs Fällen ein Sicherheitshinweis gegeben und in sieben Fällen ein Sicherheitsrisiko festgestellt wurde.

Tab. 18: SÜ im öffentlichen Bereich 2015-2017

Öffentlicher Bereich	**2015**	**2016**	**2017**	**Gesamt**
Eingeleitete SÜ	3.117	3.673	3.527	10.317
Abgeschlossene SÜ, davon	3.303	4.014	3.451	10.768
Ohne Erkenntnisse, davon	*3.211*	3.881	3.335	10.427
Sicherheitserhebliche Erkenntnisse, davon	*92*	*133*	*116*	*341*
Sicherheitshinweise	*2*	*2*	*2*	*6*
Sicherheitsrisiko	*3*	*-*	*4*	*7*

Im Gegensatz zum nichtöffentlichen Bereich ist es im öffentlichen Bereich gegenüber dem Zeitraum 2012-2014 zu einem Anstieg der im Zeitraum 2015-2017 eingeleiteten und abgeschlossenen Sicherheitsüberprüfungen von knapp 19 Prozent bzw. 28 Prozent gekommen.

Bewertung der Regelung aus Sicht des Fachreferats im BMWi

Nach Auffassung des Fachreferats habe das Änderungsgesetz 2011 zu einer Schärfung der Zielrichtung des vorbeugenden personellen Sabotageschutzes mit Blick auf bewusste (terroristische) Sabotagehandlungen geführt. Außerdem sei es zu einer Anpassung von Überprüfungsmaßnahmen, zu einer Reduzierung von unnötigen Datenerhebungen bei Betroffenen sowie zu einer Schaffung einer Ausnahmeregelung für kurzzeitige Einsätze an sicherheitsempfindlichen Stellen gekommen, die durch das Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen noch einmal erweitert wurde. Allerdings könne das BMWi-Fachreferat keine Bewertung der Ausnahmereglung vornehmen, da – nach dem Willen des Gesetzgebers – die Sabotageschutzbeauftragten in den Unternehmen mit sicherheitsempfindlichen Stellen vor Ort über die Anwendung der Ausnahmeregelung entscheiden. Eine ständige Begleitung einer sicherheitsüberprüften Person, die an einer sicherheitsempfindlichen Stelle beschäftigt sei, verursache nach Einschätzung des BMWi-Fachreferats aber in jedem Fall Kosten.
Durch die Änderungen des Änderungsgesetzes 2011 konnten ohne Sicherheitsverlust die Rechte der Betroffenen und der Datenschutz gestärkt werden und eine Harmonisierung der Personenüberprüfungen im Bereich Sabotageschutz (vpS, Luft- und Atomsicherheit) erreicht

werden. Aus Sicht des BMWi-Fachreferats konnte somit die Akzeptanz des Instruments im nichtöffentlichen Bereich erhöht werden.
Die für den nichtöffentlichen Bereich geltenden Regelungen in der SÜFV werden vom BMWi-Fachreferat als hinreichend genau angesehen, um die Wirtschaft anzusprechen, die nach Willen des Verordnungsgebers eine lebens- oder verteidigungswichtige Einrichtung im Sinne von § 1 Abs. 5 S. 1 SÜG sind. Allerdings passiere es immer wieder, dass relativ viel Zeit zwischen der Identifikation einer sicherheitsempfindlichen Stelle in einem Unternehmen und der Beantragung von SÜ-Verfahren durch die Sabotageschutzbeauftragten vergehe, da diese zuvor noch interne freiwillige Beteiligungen (z. B. Betriebsrat) vornehmen wollten. Die Streichung des § 10 Abs. 1 Nr. 2 SÜFV a. F. (sog. „Sprengstoffhersteller/-lager") habe dazu geführt, dass die Betreuung von Unternehmen eingestellt worden sei, die bislang ausschließlich aufgrund dieser Vorschrift Sicherheitsüberprüfungen durchzuführen hatten. Im Jahr 2014 seien es noch 17 Unternehmen mit eigenen sicherheitsempfindlichen Stellen und 3.330 abgeschlossenen vpS-Überprüfungen gewesen; darüber hinaus seien ca. 1.000 Personen, die über 75 Fremdfirmen an sicherheitsempfindlichen Stellen der Sprengstoffhersteller/-lager eingesetzt worden waren, nicht mehr dem vpS unterfallen. [202]
Störfallunternehmen mit erweiterten Pflichten nach der Störfallverordnung sowie Unternehmensbereiche, die diesen gleichgestellt sind (§ 10a SÜFV), müssen nur noch Sicherheitsüberprüfungen im vpS durchführen lassen, soweit der Betrieb nicht ausreichend durch organisatorische oder technische Maßnahmen gegen Eingriffe Unbefugter geschützt und dies im Sicherheitsbericht nach § 9 Störfall-Verordnung dokumentiert ist. Im Jahr 2014 betreute das BMWi 77 Störfallunternehmen[203] mit 3.566 abgeschlossenen vpS-Überprüfungen. Nach der Änderung der SÜFV seien es im Jahr 2017 noch 24 Unternehmen[204] mit 1.233 abgeschlossenen vpS-Überprüfungen.
Darüber hinaus wurde die Modifikation des § 10 Abs. 1 Nr. 1 SÜFV („Telekommunikationsunternehmen") vom BMWi-Fachreferat begrüßt, da die Zahl der Unternehmen und damit der zu überprüfende Personenkreis gegenüber der vorherigen Regelung auf das aus § 1 Abs. 5 S.1 Nr. 2 SÜG resultierende Maß begrenzt worden sei. Es gebe insgesamt rund 1.500 Unternehmen, die Übertragungswege bereitstellen. Diese seien aber nicht alle relevant für den vpS. Daher würden nun mit Blick auf § 1 Abs. 5 S. 1 Nr. 2 SÜG nur Unternehmen erfasst, die Übertragungswege für Telekommunikationsunternehmen bereitstellen oder betreiben, die Telekommunikationsdienste für mehr als 100.000 Teilnehmerinnen und Teilnehmer erbringen (§ 10 Abs. 1 Nr. 1 SÜFV i. V. m. § 1 Abs. 1 S. 1 Nr. 2 PTSG).
Das BMWi-Fachreferat geht davon aus, dass mit dem vorbeugenden personellen Sabotageschutz in den Unternehmen – da es sich um eine zusätzliche Aufgabe handele – ein zusätzlicher Aufwand verbunden sei, der sich auch noch einmal durch die SÜG-Novelle aus dem Jahr 2017 etwas erhöht habe (z. B. aufgrund einer notwendig gewordenen Anpassung der IT-Systeme zur Unterrichtung von Sabotageschutzbeauftragten durch deren Personalverwaltung). Aufgrund der Globalisierung der Märkte gebe es zudem immer mehr ausländische Unternehmen, die in Deutschland an sicherheitsempfindlichen Stellen (seS) arbeiten würden. Für diese Unternehmen würden die Regelungen und v. a. deutschsprachigen Formulare, insbesondere aufgrund der Sprachbarriere, eine besondere Herausforderung darstellen. Zugleich sei die Durchführung der Sicherheitsüberprüfungen von Personen, die im Prognosezeitraum Wohnsitze in bestimmten Staaten (z. B. solchen, die nach Feststellung des BMI als Staaten

[202] Stand: 21. August 2014.
[203] Stand: 21. August 2014.
[204] Stand: 19. Oktober 2017.

mit besonderen Sicherheitsrisiken gelten), erschwert oder unmöglich, was Unternehmensentscheidungen beeinflusse.
Vom BMWi-Fachreferat wurden zwei vpS-Bereiche genannt, in denen immer wieder Probleme auftreten würden. Zum einen werde in Ausschreibungen immer wieder eine bereits erfolgreich abgeschlossene SÜ vpS als Teilnahmevoraussetzung am Bieterwettbewerb gefordert. Dies sei jedoch unzulässig, da Unternehmen ihre Mitarbeiterinnen und Mitarbeiter nicht „auf Vorrat" einer Sicherheitsüberprüfung unterziehen dürften. Zum anderen stelle die hohe Fluktuation bei Personal von Fremdfirmen ein Problem dar. Dies führe dazu, dass Personen, die für eine Tätigkeit an einer seS überprüft würden, dann doch nicht dort eingesetzt würden, da sie nach Abschluss der Überprüfung schon nicht mehr für die Fremdfirma tätig seien oder in einem anderen (nicht sicherheitsempfindlichen) Bereich eingesetzt würden.
Optimierungsbedarf bestehe aus Sicht des BMWi-Fachreferats im Bereich der SÜFV. So verursache der neu eingefügte § 10a SÜFV aufgrund der unklaren Formulierung („soweit der Betrieb nicht ausreichend durch organisatorische oder technische Maßnahmen gegen Eingriffe Unbefugter geschützt und dies im Sicherheitsbericht nach § 9 Störfall-Verordnung dokumentiert ist") erhöhten Kommunikationsaufwand mit den betroffenen Unternehmen. Für einige Unternehmen und für einige für den Vollzug der Störfall-Verordnung zuständige Behörden sei bis heute z. T. noch unklar, wann Maßnahmen als „ausreichend" im Sinne der Vorschrift anzusehen seien. Dies führe auf allen Seiten zu Unsicherheiten, wann vpS-Überprüfungen durchzuführen seien. Zum Teil möchten auch Unternehmen, die aufgrund der neuen Vorschriften nicht mehr unter das vpS-Überprüfungsregime fallen, weiter betreut werden. Zudem sei es problematisch, dass zwei Bundesministerien (BMWi für Durchführung der Personenüberprüfungen im vpS und BMUB[205] für die Formulierung und Auslegung von § 10a SÜFV aufgrund seiner Zuständigkeit für das Störfallrecht) sowie verschiedene Kommunal- und Landesbehörden (für den Vollzug des Störfallrechts) zuständig seien. Zur Verbesserung der Situation habe das BMWi gemeinsam mit dem BMUB das Informationsblatt „Ergänzende Hinweise für Unternehmen, die den erweiterten Pflichten der Störfallverordnung unterliegen sowie für entsprechende Aufsichtsbehörden" zur Verfügung gestellt.
Insgesamt zieht das BMWi-Fachreferat im Vergleich zur vorherigen Evaluation ein positiveres Fazit mit Blick auf den vpS. Die Harmonisierung des vorbeugenden personellen Sabotageschutzes mit den Überprüfungssystemen aus Luft- und Atomsicherheit habe sich bewährt. Im Evaluationszeitraum habe es einen Fall gegeben, bei dem ein Sicherheitsrisiko festgestellt wurde. Dies zeige, dass die Sicherheitsüberprüfungen durchaus geeignete personelle Schutzmaßnahmen vor Innentätern seien. Obwohl der vpS insoweit als durchaus sinnvolles Instrument erachtet werde, könne jedoch die Frage gestellt werden, ob der Aufwand in einem angemessenen Verhältnis zum Nutzen stehe.
Nach Einschätzung des BMWi-Fachreferats halte mittlerweile die überwiegende Zahl der beim BMWi registrierten Unternehmen den vpS für ein sinnvolles Instrument. Insgesamt sei man mit dem Instrument – vor allem nach der aktuellen SÜG-Novelle – nunmehr zufrieden.
Die durch die SÜG-Novelle vorgenommen rechtlichen Änderungen wurden vom BMWi-Fachreferat insgesamt positiv bewertet, auch wenn derzeit kaum belastbare Erfahrungen mit den neuen Regelungen vorliegen würden. Als vorteilhaft wurde die Steigerung der Überprüfungsqualität durch die Einführung zusätzlicher Maßnahmen in § 12 SÜG (AZR-Auskunft, ZStV, Abfragemöglichkeit bei ausländischen Behörden, Einsichtnahme in öffentlich sichtbare Internetseiten/öffentlich sichtbare Teile sozialer Netzwerke) angesehen. Zudem wurde es von Seiten des BMWi-Fachreferats begrüßt, dass die betroffenen Personen nun zusätzlich zur

[205] Seit 14.3.2018 Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU).

Nummer des Reisepasses oder Personalausweises die ausstellende Behörde und das Ausstellungsdatum in der Sicherheitserklärung angeben müssten. Durch diese zusätzlichen Daten werde eine Identitätsprüfung bei den entsprechend ausstellenden Stellen möglich. Darüber hinaus wurde die Einfügung des § 15a SÜG positiv bewertet, da dadurch die Sabotageschutzbeauftragten im Unternehmen schneller durch die personalverwaltende Stelle über wichtige Änderungen informiert werden und somit besser als bislang in die Lage versetzt würden, ihren unverzüglichen Unterrichtungsverpflichtungen nach § 29 Abs. 1 SÜG nachzukommen. Hier bleibe allerdings abzuwarten, ob sich dies in der Praxis so bestätige.

Bewertung der Regelung aus Sicht des Fachreferats im BMI

Das BMI-Fachreferat sprach sich für eine Beibehaltung der Regelungen zum vpS im öffentlichen Bereich aus. Es sei nicht vertretbar, dass an sicherheitsrelevanten Stellen Personal eingesetzt werde, das nicht sicherheitsüberprüft sei. Genau dies würde aber geschehen, wenn die Regelungen zum vpS entfallen würden.
Die erweiterte Ausnahmeregelung werde ebenfalls positiv bewertet. Insbesondere bei kurzfristigen Tätigkeiten ermögliche die Regelung, Externe (z. B. Unternehmen) an einer sicherheitsempfindlichen Stelle zu beschäftigen, ohne eine aufwendige SÜ durchführen zu müssen. Dies bedeute weniger Arbeit für das BfV und eine geringere Belastung der betroffenen Person. Ein Nachteil der Ausnahmeregelung bestehe darin, dass die Begleitung durch sicherheitsüberprüftes Personal aufwendig sei.
Durch die Aufnahme der in § 9a SÜFV genannten Unternehmen, die z. B. am Aufbau der Netze des Bundes mitwirken, sei zudem eine Regelungslücke geschlossen worden, da diese Unternehmen lebenswichtig seien und deshalb auch vom vpS abgedeckt sein sollten.
Die Änderungen der SÜFV sowie die SÜG-Novelle hätten zudem dazu geführt, dass die Zahl und der Umfang der Sicherheitsüberprüfungen gestiegen seien. So würden im öffentlichen Bereich bei der Aktualisierung Maßnahmen wie bei einer Ü1 (Angleichung an das Vorgehen im nichtöffentlichen Bereich) und nun für alle Überprüfungsarten alle zehn Jahre Wiederholungsüberprüfungen durchgeführt.
Allerdings müsse aus Sicht des BMI-Fachreferats der vpS praktisch fortentwickelt werden. So sollten die bei einer SÜ vpS zugrunde gelegten Kriterien einer Überprüfung unterzogen werden, da eine Ü2 vpS eine geringere Wertigkeit als eine Ü2-Geheimschutz habe. Beispielsweise erfolgten bei der SÜ vps keine Abfrage von Kontakten zu ausländischen Nachrichtendiensten in der Sicherheitserklärung und keine Einbeziehung des Partners der zu überprüfenden Person. Dies führe dazu, dass nicht alle Bundesländer die SÜ vpS (Bund) in ihrem Zuständigkeitsbereich als Ü2-äquivalent anerkennen würden. Folglich komme es immer wieder zu Doppelüberprüfungen. Zudem habe es im Luftsicherheitsbereich, der als Vorlage für die Fortentwicklung der SÜ vpS diente, nunmehr eine Einführung einer allgemeinen Zuverlässigkeitsprüfung[206] gegeben, sodass auch für den vpS eine Anpassung der Kriterien geprüft werden sollte. In diesem Zusammenhang regte das BMI-Fachreferat an, ob nicht eine Vereinheitlichung der vpS-Regelungen und damit eine Reduzierung der Überprüfungsarten durch die Angleichung an den Geheimschutz sinnvoll wären.
Kein Änderungsbedarf wird hingegen bei der SÜFV gesehen. Es habe zwar in der Vergangenheit immer mal wieder Auslegungsprobleme zwischen den Ressorts gegeben. Dies sei bislang aber immer bilateral geklärt worden. Ggf. sollte darüber nachgedacht werden, die neugeschaffene Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) in § 1 der SÜFV mitaufzunehmen.

[206] Vgl. hierzu BT-Drs. 18/9752, Gesetzentwurf der Bundesregierung, Entwurf eines Ersten Gesetzes zur Änderung des Luftsicherheitsgesetzes vom 26. September 2016, S. 52-53.

Die SÜG-Novelle wurde vom BMI-Fachreferat insgesamt positiv bewertet. In § 12 SÜG wurde nun die Möglichkeit geschaffen, Abfragen in öffentlich sichtbaren Internetseiten und in öffentlich sichtbaren Teilen sozialer Netzwerke durchzuführen. Diese sei insbesondere vor dem Hintergrund der zunehmenden Bedeutung solcher Plattformen zur Darstellung der eigenen Person eine wichtige Informationsquelle. Darüber hinaus sei durch die Schaffung der Abfragemöglichkeit beim ZStV eine Anpassung an die SÜG der Bundesländer erfolgt, die diese Möglichkeit bereits vorsahen. Die Anfragen beim AZR würden bei ausländischen Personen helfen, die in der Sicherheitserklärung gemachten Angaben zu überprüfen. Die gesetzliche Regelung, bei Auslandsaufenthalten von mehr als sechs Monaten ausländische Behörden anzufragen, werde angesichts sich verändernder Karriereverläufe, bei denen Auslandsaufenthalte immer häufiger werden, als notwendig erachtet.
Ebenfalls als wichtige Neuerung werde § 15a SÜG betrachtet, da dadurch die Kommunikation zwischen der personalverwaltenden Stelle und dem Geheimschutz-/Sabotageschutzbeauftragten verbessert werde. Dieser erhalte nun schneller relevante Informationen zu Personen (z. B. Pfändungs- und Überweisungsbeschlüsse), die sicherheitsüberprüft seien.
Durch die seit der SÜG-Novelle gleichlaufende Zuständigkeit der BImA für den Geheimschutz und den vpS habe sich der Aufwand für das BMI im Bereich des vpS reduziert. Zudem führe dies zu einer Vereinfachung des Verfahrens, da die BImA nun für die Ausschreibung von Bauleistungen und die Durchführung der SÜ vpS zuständig sei. Dies trage auch dazu bei, Doppelüberprüfungen zu vermeiden.

Bewertung der Regelungen durch das BfV

Das BfV kommt insgesamt zu einer positiven Bewertung der Regelungen des vpS. Jedoch wird das Absinken der Qualität der SÜ vpS bemängelt, was dazu geführt habe, dass die LfV die Bundes SÜ vpS als nicht mehr gleichwertig zu den Landes-SÜ vpS ansehen. Dies liege vor allem daran, dass einige Aspekte nicht mehr berücksichtigt würden (z. B Angabe der Grunddaten zum Lebenspartner, der finanziellen Situation, möglicher Kontakte zu ausländischen Nachrichtendiensten). In diesem Zusammenhang wies das BfV auf einen Fall hin, bei dem das BfV durch Zufall darauf aufmerksam geworden sei, dass eine Reinigungskraft auf einer Fregatte (seS) die Verlobte eines inhaftierten IS-Anhängers gewesen sei. Dies zeige, dass die reduzierte Überprüfungstiefe nicht ausreiche, um eine umfassende Beurteilung einer Person vornehmen zu können. Kritisch angemerkt wurde dabei, dass es bei vpS-Überprüfungen alleine um die Frage des Innentäters gehe und nicht darum, die allgemeine Zuverlässigkeit einer Person zu prüfen. Der Aspekt des Herausschleusens von Informationen zur Vorbereitung einer Straftat würde nicht angemessen beachtet, da der Fokus auf möglichen Anschlagsplänen der überprüften Person liege. Nach Auffassung des BfV-Fachreferats sei es nicht verständlich, dass eine Person mit mehreren BZR-Einträgen trotzdem an einer sicherheitsempfindlichen Stelle arbeiten könne. Auch unterscheide sich die SÜ vpS im öffentlichen und nichtöffentlichen Bereich von der SÜ vpS im militärischen Sicherheitsbereich. Daher plädiere das BfV-Fachreferat für eine Vereinheitlichung der Überprüfungen – auch mit Blick auf die SÜ der Bundesländer, um hier eine wechselseitige Anerkennung zu erleichtern.
Die Zusammenarbeit mit dem BMWi habe sich in den letzten Jahren verbessert, da es weniger Konflikte als noch vor einigen Jahren gebe. Allerdings verursache die Durchführung einer SÜ vpS einen erheblichen Arbeitsaufwand. Aus Sicht des BfV könne mit einer NADIS-Abfrage und der Anforderung eines polizeilichen Führungszeugnisses mit weniger Aufwand das gleiche Sicherheitsniveau erreicht werden. Die Zusammenarbeit mit den zuständigen Stellen im öffentlichen Bereich funktioniere sehr gut. Zudem finde regelmäßig ein enger Austausch zwischen dem BfV und den zuständigen Stellen statt.

Zu den Änderungen durch die SÜG-Novelle gab das BfV an, dass eine Abfrage beim Ausländerzentralregister bisher noch nicht vorgekommen sei und aufgrund von „Kinderkrankheiten“ noch nicht erfolgen könne. Beim Zentralen Staatsanwaltschaftlichen Verfahrensregister gebe es ebenfalls technische Schwierigkeiten, die dazu geführt haben, dass noch einmal eine Abfrage bei den einzelnen Staatsanwaltschaften erfolgen müsse. Dieses Problem solle jedoch durch eine letzte technische Umstellung im Jahr 2018 gelöst werden.
Mit Blick auf die Abfragemöglichkeit bei *ausländischen Sicherheitsbehörden* verwies das BfV darauf, dass aufgrund der besonderen Wichtigkeit des Datenschutzniveaus der jeweiligen Länder genau überlegt werde, eine solche Abfrage durchzuführen. Früher seien solche Überprüfungsverfahren eingestellt worden, heute würden Ersatzmaßnahmen durchgeführt (z. B. Einholung eines polizeilichen Führungszeugnisses aus den jeweiligen Ländern). Allerdings würden dadurch nachrichtendienstliche Erkenntnisse zu der betroffenen Person fehlen. Insgesamt führe eine solche Abfrage dazu, dass das Überprüfungsverfahren aufgrund der Rückmeldungen der ausländischen Sicherheitsbehörden länger dauern würde.
Bislang noch keine Erfahrungen habe man mit der *Datengewinnung aus öffentlich zugänglichen Internetseiten bzw. öffentlich zugänglichen Teilen sozialer Netzwerke* gesammelt, da hierfür noch die technischen und personellen Voraussetzungen (Internetausstattung und Personalstellen) geschaffen werden müssten. Diese Maßnahme werde dann 2018 umgesetzt. Es gebe aber einen BMI-Erlass, der Schwerpunkte festlege, bei welchen Behörden diese Abfragemöglichkeit genutzt werden solle. Allerdings erschwere das nicht mehr erforderliche Lichtbild eine Identifizierung der jeweiligen Person im Internet.

4.11.2.1.2. Militärischer Sicherheitsbereich

Der militärische Sicherheitsbereich nimmt hinsichtlich der Organisation des Prüfungsverfahrens im vorbeugenden personellen Sabotageschutz eine Sonderstellung ein. Im Gegensatz zum nichtöffentlichen und öffentlichen Bereich ist die SÜFV für den militärischen Sicherheitsbereich nicht einschlägig. Die besonders sicherheitsempfindlichen Stellen werden im Geschäftsbereich des BMVg in direkter Anwendung der Regelung des § 1 Abs. 4 SÜG identifiziert und in Listenform im BMVg geführt. Diese Liste wird kontinuierlich angepasst. Aufgrund der Besonderheiten der militärischen Organisation (Diskontinuität der Liegenschaftszuweisung militärischer Dienststellen und Verbände) scheidet die Festlegung besonders sicherheitsempfindlicher Stellen auf der Grundlage tatbestandlicher Festlegungen im Verordnungswege, wie in der SÜFV, aus Sicht des BMVg-Fachreferates aus.
Die zuständige Stelle im militärischen Sicherheitsbereich ist zwischen den Geheimschutzbeauftragten (GB) und Sicherheitsbeauftragten (SiBe) vor Ort aufgeteilt. Dies stellt eine Besonderheit dar. Im Geschäftsbereich des BMVg gibt es insgesamt vier GB (BMVg, BAMAD, Streitkräftebasis und Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen), wobei es im BMVg nur sehr wenige und im BAMAD – aufgrund der Ü3-Pflicht für alle Mitarbeiterinnen und Mitarbeiter – überhaupt keine reinen SÜ vpS gebe. Die GB würden nur einbezogen, wenn sicherheitserhebliche Erkenntnisse festgestellt werden. In der Regel komme es dann zu einer Auflagenentscheidung. Der GB könne die Auflagen übernehmen und teile dieses dann dem SiBe mit. Falls der GB die Beurteilung des BAMAD nicht teile, gebe es ein Erörterungsverfahren. Für den Fall, dass der GB zusätzliche Informationen habe, würden diese noch einmal vom BAMAD geprüft.
Die SiBe, von denen es in der Bundeswehr zwischen 1.000 und 1.500 gibt, sind für den gesamten Bereich der militärischen Sicherheit vor Ort verantwortlich. Allerdings gibt es nur rund 130 besonders sicherheitsempfindliche Stellen im Geschäftsbereich des BMVg, sodass nur ein vergleichsweise kleiner Teil der SiBe in ihrem Verantwortungsbereich Erfahrungen mit dem

vpS gemacht hat. Neben der Zuständigkeit für das Alarmwesen und die materielle organisatorische Absicherung haben sie im vpS die Aufgabe, das Überprüfungsverfahren einzuleiten sowie nach Abschluss des Verfahrens die Einhaltung möglicher Auflagen zu überwachen.
Als eine weitere Stelle, die insgesamt für die militärische Sicherheit zuständig ist, für die die vpS-Praxis jedoch eine untergeordnete Rolle spielt, sind die Höheren Offiziere Absicherung zu nennen, von denen es acht im Geschäftsbereich des BMVg gibt. Jede Teilstreitkraft sowie die beiden zivilen Organisationsbereiche verfügen über einen solchen Offizier, der als fachlicher Vorgesetzter für die SiBe innerhalb seines Zuständigkeitsbereichs fungiert. Sie wirken bei der Identifikation sicherheitsempfindlicher Stellen mit und fungieren als Multiplikatoren im Bereich der militärischen Sicherheit und somit auch im Bereich des vpS. Etwa dreimal im Jahr treffen sich die Höheren Offiziere Absicherung, um sich über aktuelle Fragen der militärischen Sicherheit auszutauschen und sich über ein gemeinsames Vorgehen zu verständigen.
Für das militärische Personal nimmt der GB im Streitkräfteamt die Aufgaben der zuständigen Stelle wahr. Für das zivile Personal ist der GB im Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr (BAIUD-BW) zuständig. Für das ministerielle Personal des BMVg wird diese Aufgabe im BMVg selbst wahrgenommen. Der Großteil der Entscheidungen werde jedoch im nachgeordneten Bereich getroffen.
Als mitwirkende Behörde wird das BAMAD vom SiBe mit der Durchführung der SÜ beauftragt. In einem ersten Schritt prüft dieses die eingereichten Unterlagen auf Vollständigkeit, die dann an die zuständige Fachabteilung des BAMAD weitergeleitet werden. Im Anschluss daran werden die Regelanfragen gestartet (siehe Vorgehensweise im nichtöffentlichen und öffentlichen Bereich). Wie das BfV bewertet auch das BAMAD die Ergebnisse der Überprüfungsmaßnahmen in einem Votum, das dann der zuständigen Stelle als Entscheidungsgrundlage dient. Grundsätzlich können im militärischen Sicherheitsbereich – abweichend vom nichtöffentlichen und öffentlichen Bereich – folgende Ergebnisarten einer SÜ unterschieden werden:

1. *Glattabschluss (inkl. Abschlussvermerk):*

   Hierbei handelt es sich um SÜ, bei denen keine sicherheitserheblichen Erkenntnisse gewonnen wurden bzw. das BAMAD lediglich einen internen Vermerk für seine Akten erstellt hat, der jedoch nicht der zuständigen Stelle mitgeteilt wird.

2. *Einstellungen[207]:*

   Kommt es im laufenden Überprüfungsverfahren zu einem Wegfall des Überprüfungsgrunds (z. B. weil eine Person nicht mehr an einer besonders sicherheitsempfindlichen Stelle tätig sein soll), wird dieses Verfahren nicht weitergeführt, sondern eingestellt.

3. *Mitteilung sicherheitsrelevanter Erkenntnisse:*

   Hierbei handelt es sich um Erkenntnisse, die nicht für eine Auflage ausreichen, jedoch der zuständigen Stelle mitgeteilt werden. Sie spielen im Gegensatz zum nichtöffentlichen Bereich zahlenmäßig allerdings eine untergeordnete Rolle.

4. *Auflagenentscheidung:*

   Diese Form gibt es überwiegend im militärischen Sicherheitsbereich. Sie kommt dann zum Einsatz, wenn eine sicherheitliche Problemlage ohne die Feststellung eines Sicherheitsrisikos durch Auflagen, Einschränkungen und/oder personenbezogene Sicherheitshinweise beherrschbar ist. Auflagen können z. B. regelmäßige Gespräche mit dem

[207] Auch außerhalb des militärischen Sicherheitsbereichs werden Verfahrenseinstellungen vorgenommen; allerdings wurden insoweit keine statistischen Daten erhoben.

Sicherheitsbeauftragten, nach verkürzter Laufzeit angeordnete Wiederholungsüberprüfungen oder die Anzeige von Reisen in bestimmte Länder sein. Auflagen werden fallabhängig bestimmt und von der zuständigen Stelle (Geheimschutzbeauftragter) festgelegt.

5. *Sicherheitsrisiko:*

   Es liegen sicherheitserhebliche Erkenntnisse i. S. d. § 5 SÜG vor, die nach Bewertung des Einzelfalls dazu führen, dass betroffene Person die Tätigkeit an einer besonders sicherheitsempfindlichen Stelle nicht aufnehmen bzw. dort nicht weiterbeschäftigt werden darf.

Nach Angaben des BAMAD würden beim Großteil der Fälle keine sicherheitserheblichen Erkenntnisse festgestellt. Für eine SÜ vpS, die zu einem „Glattabschluss"-Ergebnis führe, sei der Aufwand vergleichsweise gering, da das Verfahren weitgehend automatisiert durchgeführt werde.
Bei sicherheitserheblichen Erkenntnissen dauere das Verfahren hingegen länger (zwischen drei Monaten und vier Jahren). In diesen Fällen erfolge eine Einzelfallprüfung. Insbesondere die Befragung der betroffenen Personen sei sehr aufwendig. Es gebe immer wieder Fälle, in denen die betroffenen Personen bei der Beantwortung der Fragen auf eine „Salamitaktik" setzen und dadurch das Verfahren verzögern würden. Die Zahl der Fälle mit sicherheitserheblichen Erkenntnissen sei nach Einschätzung des BAMAD in den letzten Jahren deutlich gestiegen. Dies liege auch daran, dass viele Bewerberinnen und Bewerber familiäre Bindungen zu Staaten i. S. d. § 13 Abs. 1 Nr. 17 SÜG (z. B. Russland) hätten.
Falls die SÜ noch nicht abgeschlossen ist, die betreffende Person jedoch für eine bestimmte Aufgabe benötigt wird, kann der Zugang zu einer besonders sicherheitsempfindlichen Stelle auf der Grundlage des § 9 Abs. 2 SÜG zugelassen werden (z. B. bei zeitlich begrenztem Einsatz und mit Begleitung). Im militärischen Sicherheitsbereich ist eine ständige Begleitung durchaus an nicht wenigen Stellen möglich. Z.T. ist auch der Einsatz einer Person bei Vorlage eines vorläufigen Ergebnisses möglich.
Insgesamt wurden zwischen Januar 2015 und Dezember 2017 45.673 SÜ im militärischen Sicherheitsbereich eingeleitet. Im gleichen Zeitraum wurden 50.505 SÜ abgeschlossen. Rund 94 Prozent der abgeschlossenen SÜ waren sog. Glattabschlüsse (inkl. Abschlussvermerk), d. h. es gab keinerlei sicherheitserheblichen Hinweise. In etwas mehr als einem Prozent der Fälle wurden sicherheitserhebliche Erkenntnisse gewonnen, während es in mehr als drei Prozent der Fälle zu Auflagenentscheidungen kam. In 402 Fällen wurde im Rahmen der SÜ ein Sicherheitsrisiko festgestellt. In 132 Fällen wurden die Überprüfungsverfahren eingestellt.

Tab. 19: SÜ im militärischen Sicherheitsbereich 2015-2017

	2015	2016	2017	Gesamt
Eingeleitete SÜ	**16.589**	**15.644**	**13.440**	**45.673**
Abgeschlossene SÜ, davon	**20.486**	**16.113**	**13.906**	**50.505**
Glattabschlüsse (inkl. AV)	19.613	15.064	13.023	47.700
Einstellungen[208]	-	-	132	132
Sicherheitserhebliche Erkenntnisse	182	296	108	586
Auflagenentscheidungen	539	621	525	1.685
Sicherheitsrisiko	152	132	118	402

Bewertung der Regelung durch das BMVg-Fachreferat und das BAMAD

Aus Sicht des BMVg-Fachreferats haben sich die Regelungen zum vorbeugenden personellen Sabotageschutz bewährt. Die Notwendigkeit der Beibehaltung ergebe sich zudem aus der erhöhten Sicherheitslage in der Bundeswehr. Sollte der vpS abgeschafft werden, würde sich das BMVg für bereichsspezifische Vorschriften zum vpS aussprechen.
Gewisse Anwendungsunsicherheiten würden sich in Bezug auf § 1 Abs. 4 SÜG ergeben, da hier von „militärischem Sicherheitsbereich“ gesprochen werde. Dieser Begriff werde jedoch im militärischen Kontext anders verwendet, da hier jede Kaserne einen militärischen Sicherheitsbereich darstelle. Übersehen werde dabei immer wieder, dass das SÜG nur bei besonders sicherheitsempfindlichen Stellen zur Anwendung kommen solle.
Mit der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) zeigte sich das BMVg-Fachreferat insgesamt zufrieden, da sie eine höhere Flexibilität in den angestrebten Bereichen, d. h. vor allem bei Reparaturarbeiten durch Fremdfirmen und beim Einsatz von militärischem Personal, biete. Allerdings bedürfe jede Ausnahme einer Einzelfallentscheidung und füge sich nur bedingt in das militärische System klarer Befehle ein.
Wie sich die für alle neu eingestellten Soldatinnen und Soldaten eingeführte einfache SÜ (Ü1) auf den vpS auswirken werde, könne abschließend noch nicht beurteilt werden, da die Regelung erst seit Juli 2017 in Kraft ist. Das BMVg-Fachreferat rechne aber damit, dass die Probleme, die sich aus einer fehlenden SÜ ergeben (z. B. Nicht-Besetzung einer Stelle, die einer SÜ vpS bedarf), in Zukunft weniger ins Gewicht fallen werden. Denn alle gemäß Soldatengesetz überprüften Soldatinnen und Soldaten könnten ihre Tätigkeit direkt – wenn auch vorläufig – aufnehmen, während die SÜ vpS parallel durchgeführt werde, ohne dass es einer Ausnahmeregelung bedarf (siehe § 15 SÜG). Ebenfalls schwer absehbar sei momentan, wie sich die neu eingeführte SÜ auf die Prüfdauern bereits bestehender SÜ-Arten auswirken werde.
Optimierungsbedarf im Bereich des vpS gebe es nach Aussage des BMVg-Fachreferats derzeit nicht.
Nach Einschätzung des BAMAD habe sich das Instrument der Sicherheitsüberprüfung im Bereich des vpS bewährt und sollte daher beibehalten werden, da es eine notwendige Ergänzung des materiellen Sabotageschutzes darstelle. Allerdings passe das SÜG nicht für die Bundeswehr, weshalb sich die Frage nach einem ressortspezifischen SÜG stelle. Darüber hinaus

[208] Diese Abschlussart wurde erstmalig in der Statistik für das Jahr 2017 separat ausgewiesen. Außerhalb des militärischen Sicherheitsbereichs wurden keine statistischen Daten über Einstellungen erhoben.

sei es ein Problem, dass die SiBe oftmals keine ausreichende Ausbildung/Qualifizierung bekommen würden und nicht ausreichend Zeit für die Beschäftigung mit Fragen des vpS hätten. Aus diesem Grund plädierte das BAMAD für eine bessere Qualifizierung der SiBe, aber auch der Dienststellenleiter.
Doppelüberprüfungen seien kein Problem mehr, da – sollte es zu einer Einleitung einer Ü2 Geheimschutz kommen – beide Verfahren zusammengezogen würden. Aufgrund der Rechtsprechung des Bundesverwaltungsgerichts habe sich der Aufwand bei der Durchführung einer SÜ insgesamt erhöht. Ein gesteigerter Aufwand bei der Begründung ergebe sich bei Voten, welche die Feststellung eines Sicherheitsrisikos vorschlagen. In diesen Fällen komme es in der Folge zur Anhörung der betroffenen Person. Hierfür müsse das Votum Aussagen zu den Punkten enthalten, die nach der Rechtsprechung des Bundesverwaltungsgerichts als entscheidungserheblich und damit darlegungsbedürftig seien.
Aus Sicht des BAMAD sei es sachgerecht, dass es aufgrund der unterschiedlichen Bewertungsmaßstäbe unterschiedliche Ergebnisse bei einer SÜ Geheimschutz und einer SÜ vpS geben könne. So könne es passieren, dass bei der SÜ Geheimschutz ein Sicherheitsrisiko festgestellt werde und die SÜ vpS lediglich eine Erteilung von Auflagen vorsehe.

4.11.2.2. Zentrale Ergebnisse der Befragung der Sabotageschutz- bzw. Sicherheitsbeauftragten im öffentlichen, nichtöffentlichen und militärischen (Sicherheits-)Bereich

4.11.2.2.1. Nichtöffentlicher Bereich

Um Erkenntnisse zur den Erfahrungen mit der Umsetzung des vorbeugenden personellen Sabotageschutzes (vpS) – insbesondere zur Nutzung der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) sowie zur Einschätzung des mit dem vpS verbundenen Aufwands – im nichtöffentlichen Bereich gewinnen zu können, wurde im Mai/Juni 2017 eine onlinegestützte Befragung der Sabotageschutzbeauftragten der beim BMWi registrierten Unternehmen durchgeführt. Hierzu wurde in enger Abstimmung mit dem für den vpS zuständigen Fachreferat im BMWi ein Online-Fragebogen für drei unterschiedliche Unternehmenstypen (Unternehmen mit eigener sicherheitsempfindlicher Stelle, Fremdfirmen[209] sowie Sabotageschutz-Dienstleister[210]) entwickelt. Der Fragebogen bestand aus vier Teilen. Der erste Teil fungierte als Filter, um die Sabotageschutzbeauftragten zum richtigen unternehmensspezifischen Teil weiterleiten zu können. Darüber hinaus erhielt er bereits erste unternehmensbezogene Fragen (z. B. Unternehmensgröße, BMWi-Betriebsnummer(n)).
Der Fragebogen-Link mit Passwort sowie ein Informationsschreiben wurden vom BMWi per Post an 1.097 Unternehmen verschickt, die vier Wochen Zeit hatten, den Fragebogen elektronisch zu beantworten. Anfang Juni 2017 wurden die Unternehmen, die sich bis dato noch nicht an der Befragung beteiligt hatten, noch einmal aufgefordert, den Fragebogen innerhalb von zwei Wochen zu beantworten. Anfang Juli 2017 wurde der Fragebogen-Link deaktiviert, sodass ab diesem Zeitpunkt keine Teilnahme mehr möglich war.

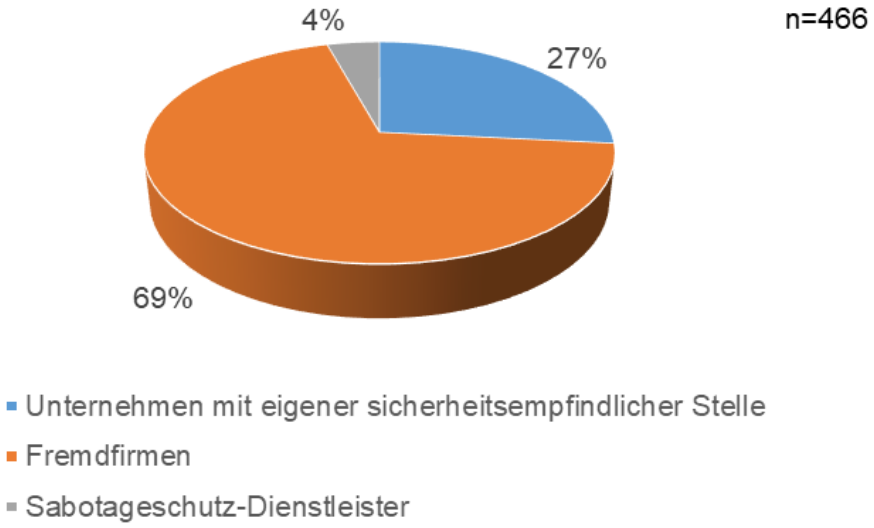
Rücklauf

Insgesamt beantworteten 466 Unternehmen den elektronischen Fragebogen vollständig. Der Großteil der Sabotageschutzbeauftragten war in Fremdfirmen tätig (322), während 27 Prozent der Befragten in Unternehmen mit eigener sicherheitsempfindlicher Stelle (124) arbeiteten.

[209] Hierbei handelt es sich z. B. um Wartungs- und Reinigungsfirmen, die ihr Personal an sicherheitsempfindlichen Stellen anderer Unternehmen einsetzen.
[210] Hierbei handelt es sich um Dienstleister, die die Aufgaben des vpS für andere Unternehmen wahrnehmen.

Vier Prozent der Befragten nahmen die Aufgaben des vpS als sog. Sabotageschutz-Dienstleister für andere Unternehmen wahr (20).

Abb. 11: Anteil der Unternehmen nach Unternehmensart



Zehn Fremdfirmen und elf Unternehmen mit einer eigenen sicherheitsempfindlichen Stelle gaben zudem an, dass sie die Aufgabe des Sabotageschutzbeauftragten auch für insgesamt 37 weitere Unternehmen wahrnehmen.
Eine Rücklaufquote lässt sich nur für die beim BMWi registrierten Unternehmen insgesamt ermitteln, nicht jedoch für die drei Unternehmenstypen, da keine Statistik darüber existiert, wie hoch die Gesamtzahl in der jeweiligen Gruppe ist. Für den gesamten nichtöffentlichen Bereich betrug die Rücklaufquote 42,5 Prozent.
Da die Fragen – je nach Unternehmenstyp – variierten, werden im Folgenden die Auswertungsergebnisse differenziert nach Fremdfirmen, Unternehmen mit eigener sicherheitsempfindlicher Stelle und Sabotageschutz-Dienstleistern dargestellt:

Fremdfirmen

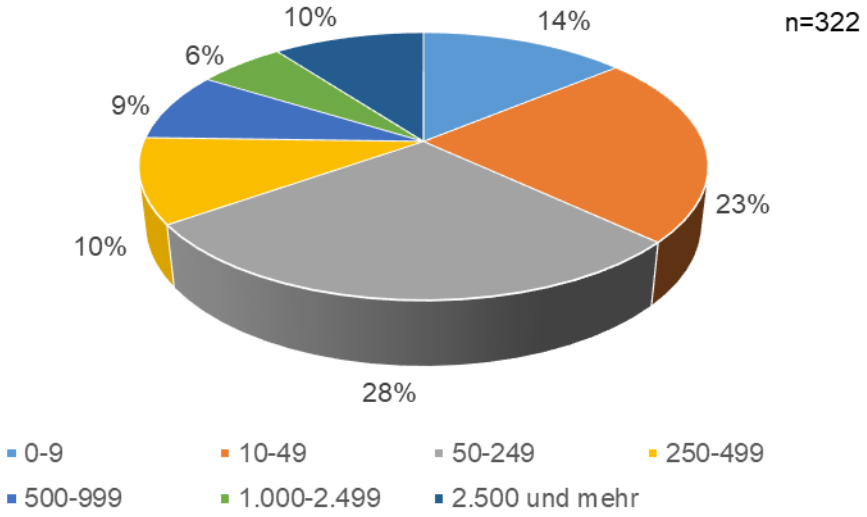
Der Großteil der befragten Sabotageschutzbeauftragten gab an, dass ihr Unternehmen Personal an verteidigungswichtige Einrichtungen (213) entsendet. Darüber hinaus wurden Telekommunikationsunternehmen (69) und Unternehmen mit Leitstellen für das überregionale Elektrizitätsübertragungsnetz (64) genannt. Hingegen spielten Unternehmen mit erweiterten Pflichten nach der Störfall-Verordnung (31), mit dem Aufbau oder Betrieb des Digitalfunks BOS beauftragte Unternehmen (29), Eisenbahn-/Untergrundbahnunternehmen (21) sowie Gefahrgutunternehmen mit Sicherungsplänen nach UA 1.10.3.2 ADR, RID oder ADN (18) eine untergeordnete Rolle. Somit wurden alle in der SÜFV genannten Unternehmen in der Befragung berücksichtigt:

Tab. 20: Art der Unternehmen, in welche die Fremdfirmen Personal entsenden, nach SÜFV-Typisierung

Art der Unternehmen, in welche die Fremdfirmen Personal entsenden	**Anzahl Nennungen** (Mehrfachnennungen möglich)
Unternehmen, das mit dem Aufbau oder Betrieb des Digitalfunks BOS beauftragt ist (§ 9a Nummer 1 SÜFV)	29
Telekommunikationsunternehmen (§ 10 Absatz 1 Nummer 1 SÜFV)	69
Unternehmen mit Leitstellen für das überregionale Elektrizitätsübertragungsnetz (§ 10 Absatz 1 Nummer 2 SÜFV)	64
Verteidigungswichtige Einrichtung (§ 10 Absatz 2 SÜFV)	213
Unternehmen mit erweiterten Pflichten nach der Störfall-Verordnung (§ 10a SÜFV)	31
Eisenbahn-/Untergrundbahnunternehmen (§ 11 Nummer 1 SÜFV)	21
Gefahrgutunternehmen mit Sicherungsplänen nach UA 1.10.3.2 ADR, RID oder ADN (§ 11 Nummer 2 SÜFV)	18
Gesamt	**445**

Betrachtet man die Größenstruktur der befragten Fremdfirmen, zeigt sich, dass sich alle Unternehmensgrößen an der Befragung beteiligten. Etwa zwei Drittel der Fremdfirmen hatten weniger als 250 Mitarbeiterinnen und Mitarbeiter. Jedes fünfte Unternehmen beschäftigte zwischen 250 und 999 Mitarbeiterinnen und Mitarbeitern, während 16 Prozent der befragten Fremdfirmen mehr als 999 Mitarbeiterinnen und Mitarbeiter hatten.

Abb. 12: Unternehmensgröße der Fremdfirmen



Mehr als die Hälfte der Sabotageschutzbeauftragten der Fremdfirmen charakterisierten die Hauptbeschäftigung, die sie in ihrem Unternehmen ausüben, als eine Beschäftigung mit Führungsaufgaben oder schwierigen, komplexen Tätigkeiten (177). 37 Prozent gaben an, dass sie eine Beschäftigung mit qualifizierten Fachtätigkeiten ausüben (118), während es sich bei acht Prozent der Sabotageschutzbeauftragten um eine Beschäftigung mit ausführenden Tätigkeiten nach allgemeiner Anweisung handelte.

Unternehmen mit eigener sicherheitsempfindlicher Stelle

Am häufigsten gaben die Sabotageschutzbeauftragten an, dass sie in einem Gefahrgutunternehmen mit Sicherungsplänen nach UA 1.10.3.2 ADR, RID oder ADN (53) beschäftigt sind. Darüber hinaus arbeiteten die Befragten in Unternehmen mit erweiterten Pflichten nach der Störfall-Verordnung (34)[211] sowie in verteidigungswichtigen Einrichtungen (31). Telekommunikationsunternehmen (15)[212], Unternehmen mit Leitstellen für das überregionale Elektrizitätsübertragungsnetz (9)[213] sowie Eisenbahn-/Untergrundbahnunternehmen (3) wurden deutlich seltener genannt.

[211] Zum Zeitpunkt der Umfrage befanden sich 24 entsprechende Unternehmen in der Betreuung durch BMWi. Im Anschreiben wurde darum gebeten, dass nur die oder der Sabotageschutzbeauftragte (kein/e Vertreter/in) die Umfrage ausfüllt, sodass nur eine Rückmeldung pro betreutem Unternehmen erfolgt.
[212] Zum Zeitpunkt der Umfrage befanden sich acht entsprechende Unternehmen in der Betreuung durch BMWi. Im Anschreiben wurde darum gebeten, dass nur die oder der Sabotageschutzbeauftragte (kein/e Vertreter/in) die Umfrage ausfüllt, sodass nur eine Rückmeldung pro betreutem Unternehmen erfolgt.
[213] Zum Zeitpunkt der Umfrage befanden sich vier entsprechende Unternehmen in der Betreuung durch BMWi. Im Anschreiben wurde darum gebeten, dass nur die oder der Sabotageschutzbeauftragte (kein/e Vertreter/in) die Umfrage ausfüllt, sodass nur eine Rückmeldung pro betreutem Unternehmen erfolgt.

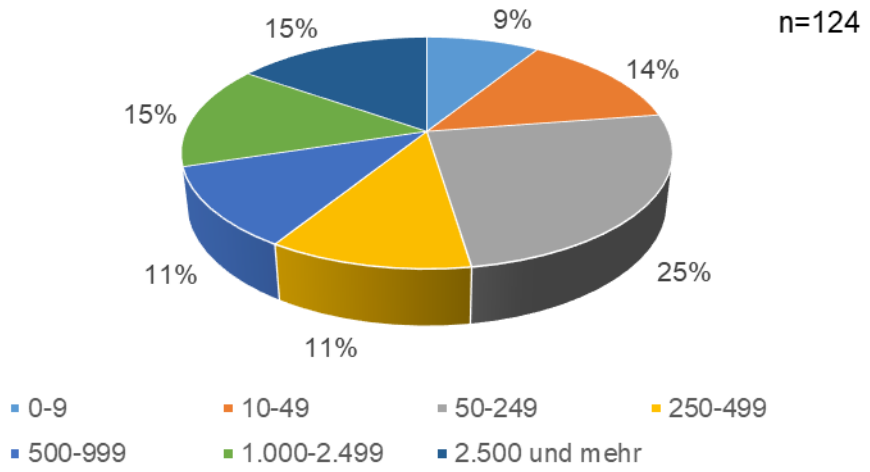
Tab. 21: Art der Unternehmen mit eigener sicherheitsempfindlicher Stelle nach SÜFV-Typisierung

Art der Unternehmen mit eigener sicherheitsempfindlicher Stelle	Anzahl
Unternehmen, das mit dem Aufbau oder Betrieb des Digitalfunks BOS beauftragt ist (§ 9a Nummer 1 SÜFV)	8[214]
Telekommunikationsunternehmen (§ 10 Absatz 1 Nummer 1 SÜFV)	15
Unternehmen mit Leitstellen für das überregionale Elektrizitäts-übertragungsnetz (§ 10 Absatz 1 Nummer 2 SÜFV)	9
Verteidigungswichtige Einrichtung (§ 10 Absatz 2 SÜFV)	31
Unternehmen mit erweiterten Pflichten nach der Störfall-Verordnung (§ 10a SÜFV)	34
Eisenbahn-/Untergrundbahnunternehmen (§ 11 Nummer 1 SÜFV)	3
Gefahrgutunternehmen mit Sicherungsplänen nach UA 1.10.3.2 ADR, RID oder ADN (§ 11 Nummer 2 SÜFV)]	53
Gesamt	**153**

Betrachtet man die Größenstruktur der befragten Unternehmen mit eigener sicherheitsempfindlicher Stelle, zeigte sich, dass sich – wie auch schon bei den Fremdfirmen – alle Unternehmensgrößen an der Befragung beteiligten. Fast die Hälfte der Unternehmen hatte weniger als 250 Mitarbeiterinnen und Mitarbeiter. Etwas mehr als jedes fünfte Unternehmen beschäftigte zwischen 250 und 999 Mitarbeiterinnen und Mitarbeitern, während rund 30 Prozent der befragten Fremdfirmen mehr als 999 Mitarbeiterinnen und Mitarbeiter hatten.

[214] Zum Zeitpunkt der Umfrage befanden sich vier entsprechende Unternehmen in der Betreuung durch BMWi. Im Anschreiben wurde darum gebeten, dass nur die oder der Sabotageschutzbeauftragte (kein/e Vertreter/in) die Umfrage ausfüllt, sodass nur eine Rückmeldung pro betreutem Unternehmen erfolgt.

Abb. 13: Größe der Unternehmen mit eigener sicherheitsempfindlicher Stelle



Mehr als 60 Prozent der Sabotageschutzbeauftragten in Unternehmen mit eigener sicherheitsempfindlicher Stelle charakterisierten die Hauptbeschäftigung, die sie in ihrem Unternehmen ausüben, als eine Beschäftigung mit Führungsaufgaben oder schwierigen, komplexen Tätigkeiten (79). 33 Prozent der Befragten gaben an, dass sie eine Beschäftigung mit qualifizierten Fachtätigkeiten ausüben (41), während es sich bei lediglich drei Prozent der Sabotageschutzbeauftragten um eine Beschäftigung mit ausführenden Tätigkeiten nach allgemeiner Anweisung handelte (4).

Sabotageschutz-Dienstleister

Die Sabotageschutz-Dienstleister wurden danach gefragt, für welche Art von Unternehmen sie die Aufgabe des Sabotageschutzbeauftragten wahrnehmen. Dabei zeigte sich, dass die Befragten schwerpunktmäßig für Fremdfirmen, die Personal an Unternehmen mit sicherheitsempfindlichen Stellen (15) entsenden. In etwas geringerem Umfang stellen Unternehmen mit eigener sicherheitsempfindlicher Stellen (11) ein Einsatzgebiet für die befragten Sabotageschutz-Dienstleister dar.
Auch bei den SÜFV-Typisierungen lässt sich kein eindeutiger Schwerpunkt erkennen. Am häufigsten übernahmen die Befragten die Aufgabe für verteidigungswichtige Einrichtungen (5), gefolgt von Gefahrgutunternehmen mit Sicherungsplänen nach UA 1.10.3.2 ADR, RID oder ADN, Fremdfirmen, die Personal an Telekommunikationsunternehmen entsenden, Fremdfirmen, die Personal in verteidigungswichtige Einrichtungen entsenden, sowie Fremdfirmen, die Personal an Eisenbahn-/Untergrundbahnunternehmen entsenden (je 3). Des Weiteren wurden die Befragten für Fremdfirmen, die Personal an Unternehmen entsenden, die mit dem Aufbau oder Betrieb des Digitalfunks BOS beauftragt sind, für Fremdfirmen, die Personal an Unternehmen mit Leitstellen für das überregionale Elektrizitätsübertragungsnetz entsenden, sowie für Fremdfirmen, die Personal an Unternehmen mit erweiterten Pflichten nach der Störfall-Verordnung entsenden (je 2), als Sabotageschutz-Dienstleister tätig. Schließlich wurde die Aufgabe des Sabotageschutzbeauftragten für ein Unternehmen mit Leitstellen für

das überregionale Elektrizitätsübertragungsnetz, für ein Unternehmen mit erweiterten Pflichten nach der Störfall-Verordnung sowie für ein Eisenbahn-/Untergrundbahnunternehmen wahrgenommen.[215]

Tab. 22: Art der Unternehmen, für die die Aufgabe des Sabotageschutzbeauftragten wahrgenommen wird

Art der Unternehmen, für die die Aufgabe des Sabotageschutzbeauftragten wahrgenommen wird	**Anzahl**
Unternehmen mit eigener sicherheitsempfindlicher Stelle	**11**
Unternehmen, das mit dem Aufbau oder Betrieb des Digitalfunks BOS beauftragt ist (§ 9a Nummer 1 SÜFV)	-
Telekommunikationsunternehmen (§ 10 Absatz 1 Nummer 1 SÜFV)	-
Unternehmen mit Leitstellen für das überregionale Elektrizitätsübertragungsnetz (§ 10 Absatz 1 Nummer 2 SÜFV)	1
Verteidigungswichtige Einrichtung (§ 10 Absatz 2 SÜFV)	5
Unternehmen mit erweiterten Pflichten nach der Störfall-Verordnung (§ 10a SÜFV)	1
Eisenbahn-/Untergrundbahnunternehmen (§ 11 Nummer 1 SÜFV)	1
Gefahrgutunternehmen mit Sicherungsplänen nach UA 1.10.3.2 ADR, RID oder ADN (§ 11 Nummer 2 SÜFV)]	3
Fremdfirmen gesamt	**15**
Fremdfirmen, die Personal an Unternehmen entsenden, die mit dem Aufbau oder Betrieb des Digitalfunks BOS beauftragt sind	2
Fremdfirmen, die Personal an Telekommunikationsunternehmen entsenden	3
Fremdfirmen, die Personal an Unternehmen mit Leitstellen für das überregionale Elektrizitätsübertragungsnetz entsenden	2
Fremdfirmen, die Personal in verteidigungswichtige Einrichtungen entsenden	3
Fremdfirmen, die Personal an Unternehmen mit erweiterten Pflichten nach der Störfall-Verordnung entsenden	2

[215] Diese Sachverhalte wurden im Rahmen der Befragung so vorgetragen. Sie sind dem für die Firmenbetreuung zuständigen BMWi jedoch nicht bekannt.

Fremdfirmen, die Personal an Eisenbahn-/Untergrundbahnunternehmen entsenden	3
Fremdfirmen, die Personal an Gefahrgutunternehmen mit Sicherungsplänen nach UA 1.10.3.2 ADR, RID oder ADN entsenden	-
Gesamt	**26**

Mehr als 70 Prozent der Sabotageschutz-Dienstleister charakterisierten die Hauptbeschäftigung, die sie in ihrem Unternehmen ausüben, als eine Beschäftigung mit Führungsaufgaben oder schwierigen, komplexen Tätigkeiten (14). Ein Viertel der Befragten gab an, dass sie eine Beschäftigung mit qualifizierten Fachtätigkeiten ausüben (5), während es sich bei einem Sabotageschutz-Dienstleister um eine Beschäftigung mit ausführenden Tätigkeiten nach allgemeiner Anweisung handelte.

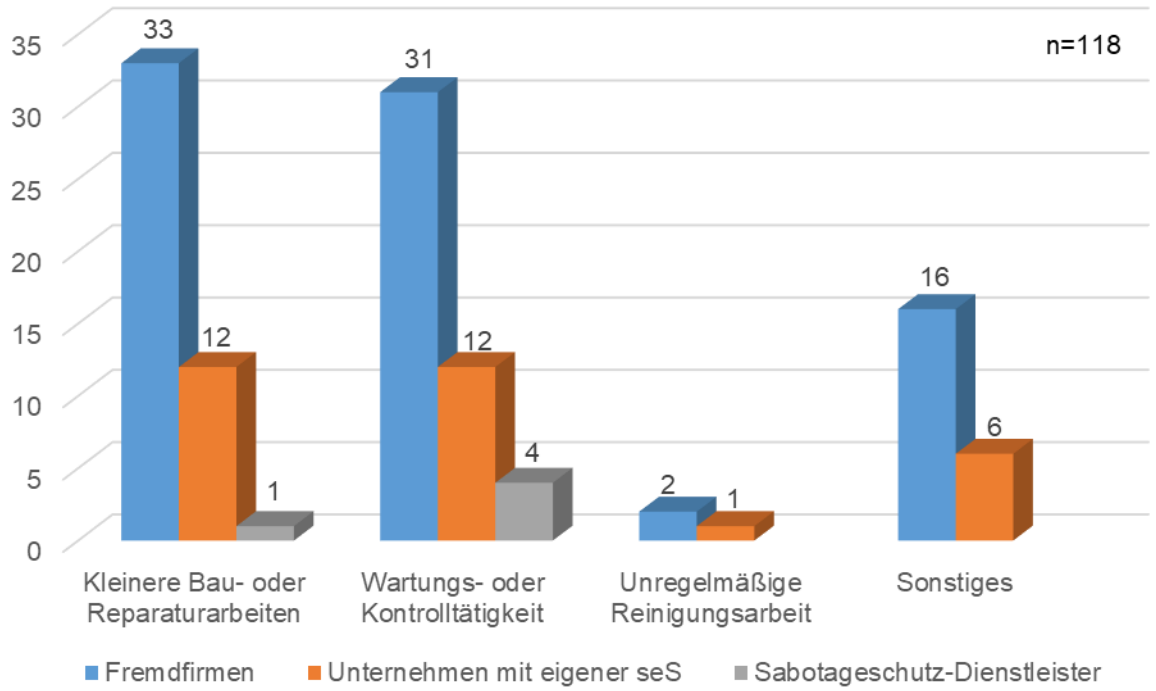
Identifikation sicherheitsempfindlicher Stellen in den Unternehmen

Zunächst ist darauf hinzuweisen, dass nur die Sabotageschutzbeauftragten der Unternehmen mit eigener sicherheitsempfindlicher Stelle sowie die Sabotageschutz-Dienstleister danach gefragt wurden, ob sie an der Identifikation oder Neufassung einer sicherheitsempfindlichen Stelle im Rahmen ihrer Tätigkeit mitgewirkt haben, da nur sie hierzu eine Einschätzung abgeben konnten. Sabotageschutzbeauftragte, die in Fremdfirmen tätig sind, können hierzu keine Angaben machen, da die Identifikation einer sicherheitsempfindlichen Stelle in den Zuständigkeitsbereich des jeweiligen Unternehmens fällt, das nach Feststellung in der SÜFV lebens- oder verteidigungswichtige Einrichtung ist. 43 Prozent der Befragten (62) gaben an, dass sie an der Identifikation oder Neufassung einer solchen Stelle mitgewirkt haben, während etwa 57 Prozent (82) dies verneinten. Insgesamt verlief das Verfahren problemlos. Lediglich sieben Sabotageschutzbeauftragte aus Unternehmen mit eigenen sicherheitsempfindlichen Stellen wiesen auf Probleme hin, die im Zusammenhang mit der Identifikation oder Neufassung aufgetreten sind.

Nutzung und Bewertung der zeitlich erweiterten Ausnahmereglung (§ 9 Abs. 2 Nr. 2 SÜG)

Etwa 81 Prozent der Sabotageschutzbeauftragten (378) wiesen darauf hin, dass sie seit 2016 keinen Gebrauch von der zeitlich erweiterten Ausnahmeregelung gemäß § 9 Abs. 2 Nr. 2 SÜG gemachten haben. Dagegen nutzten knapp 19 Prozent der Befragten (88) diese Möglichkeit bei insgesamt 828 Mitarbeiterinnen und Mitarbeitern. Von der Ausnahmeregelung profitierten die drei Unternehmenstypen in unterschiedlichem Ausmaß: Unternehmen mit eigener sicherheitsempfindlicher Stelle (560 Mitarbeiterinnen und Mitarbeiter), Fremdfirmen (259 Mitarbeiterinnen und Mitarbeiter) sowie Sabotageschutz-Dienstleister (neun Mitarbeiterinnen und Mitarbeiter).
Die Mitarbeiterinnen und Mitarbeiter, bei denen von einer SÜ vpS abgesehen wurde, da sie ständig begleitet wurden, wurden vor allem für Wartungs- und Kontrolltätigkeiten (47) sowie für kleinere Bau- und Reparaturarbeiten (46) eingesetzt. Unregelmäßige Reinigungstätigkeiten (3) spielten lediglich eine untergeordnete Rolle für die Nutzung der Ausnahmeregelung. Darüber hinaus wurden in 22 Fällen weitere Gründe genannt.

Abb. 14: Anwendungsbereiche der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG)



Von den Sabotageschutzbeauftragten, welche die zeitlich erweiterte Ausnahmeregelung seit 2016 noch nicht genutzt haben, wurden folgende Gründe genannt:

- Es gab keinen Anwendungsbereich, der eine Ausnahme ermöglicht hätte (147).
- Alle Mitarbeiter/innen in meinem Unternehmen werden sicherheitsüberprüft, damit sie flexibel eingesetzt werden können (59).
- Es hätte zwar ggf. Fälle gegeben, in denen man davon hätte Gebrauch machen können. Allerdings war mir nicht bekannt, dass es die Ausnahmeregelung gibt (40).
- Wartungs- oder Kontrolltätigkeiten werden durch Personal vorgenommen, das ohnehin dauerhaft an der sicherheitsempfindlichen Stelle beschäftigt ist (39).
- Die Ausnahmeregelung war mir nicht bekannt (25).
- Bau- oder Reparaturarbeiten dauern länger als vier Wochen (14).
- In den von uns betreuten Unternehmen werden grundsätzlich alle Personen, die an einer sicherheitsempfindlichen Stelle arbeiten, sicherheitsüberprüft (9).
- Das Abstellen einer sicherheitsüberprüften Person, die die nicht überprüfte Person ständig begleitet, ist zu teuer (9).
- Sonstiges (45).

Die Sabotageschutzbeauftragten wurden ebenfalls gefragt, wie sie die Relevanz der zeitlich erweiterten Ausnahmeregelung gemäß § 9 Abs. 2 Nr. 2 SÜG einschätzten. Auffällig ist, dass etwa 42 Prozent der Befragten diese für vollkommen bzw. eher irrelevant hielten. Knapp 15 Prozent bewerteten die Ausweitung als teilweise relevant, während nur etwas mehr als 17 Prozent der Auffassung waren, dass sie sehr bzw. eher relevant für das jeweilige Unternehmen ist.

Tab. 23: Bewertung der Relevanz der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich[216]

Relevanz Ausnahme-regelung	FF	in %	U. m. eig. seS	in %	Sab-D.	in %	Gesamt	in %
Sehr relevant	28	8,7	6	4,8	1	5,0	35	7,5
Eher relevant	32	9,9	14	11,3	-	-	46	9,9
Teils/Teils	49	15,2	15	12,1	4	20,0	68	14,6
Eher irrelevant	90	28,0	37	29,8	2	10,0	129	27,7
Vollkommen irrelevant	37	11,5	25	20,2	4	20,0	66	14,2
Keine Angabe	86	26,7	27	21,8	9	45,0	122	26,2
Gesamt	**322**	**100,0**	**124**	**100,0**	**20**	**100,0**	**466**	**100,0**

Darüber hinaus wurden die Sabotageschutzbeauftragten gefragt, ob sie die Ausweitung der Ausnahmeregelung für ausreichend halten. Knapp 87 Prozent der Befragten hielten diese für ausreichend. Lediglich rund 13 Prozent der Sabotageschutzbeauftragten waren der Meinung, dass die erweiterte Ausnahmenregelung nicht ausreichend ist.

Tab. 24: Bewertung der zeitlichen erweiterten Ausnahmeregelung als ausreichend durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich

§ 9 Abs. 2 Nr. 2 SÜG ausrei-chend	FF	in %	U. m. eig. seS	in %	Sab-D.	in %	Gesamt	in %
Ja	275	85,4	109	87,9	20	100	404	86,7
Nein	47	14,6	15	12,1	-	-	62	13,3
Gesamt	322	100,0	124	100,0	20	100	466	100,0

Nutzung der Anerkennensregelung (§ 2 Abs. 1 S. 5 SÜG)

Die Sabotageschutzbeauftragten wurden auch danach gefragt, wie oft seit 2015 die Anerkennensregelung gemäß § 2 Abs. 1 S. 5 SÜG zur Anwendung kam und sie von der Einleitung einer SÜ vpS absehen konnten, da bereits eine noch gültige und gleich- oder höherwertige Überprüfung aus dem Geheimschutz, der Luft- oder Atomsicherheit vorlag.
Etwa drei Viertel der Befragten (352) gab an, von dieser Anerkennensregelung bislang keinen Gebrauch gemacht zu haben. Knapp ein Viertel der Sabotageschutzbeauftragten (114) nutzte

[216] **FF**=Fremdfirmen, **U. m. eig. seS**= Unternehmen mit eigener sicherheitsempfindlicher Stelle; **Sab-D.**=Sabotageschutz-Dienstleister

diese Möglichkeit bei insgesamt 5.103 Personen, wobei der Großteil der Mitarbeiterinnen und Mitarbeiter (4.359) in Unternehmen mit eigener sicherheitsempfindlicher Stelle tätig war. Anzumerken ist in diesem Zusammenhang jedoch, dass ein Unternehmen angab, auf die Anerkennensregelung für 3.000 Personen zurückgegriffen zu haben. Des Weiteren konnte bei 740 Mitarbeiterinnen und Mitarbeitern von Fremdfirmen gemäß § 2 Abs. 1 S.5 SÜG auf eine SÜ vpS verzichtet werden, während es bei den Sabotageschutz-Dienstleistern vier Personen waren.

Tab. 25: Anwendung der Anerkennensregelung (§ 2 Abs. 1 S. 5 SÜG) durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich

Anwendung Anerkennensregelung (§ 2 Abs. 1 S. 5 SÜG)	FF	U. m. eig. seS	Sab-D.	Gesamt	in %
Nein	248	87	17	352	75,5
Ja und zwar bei:	74[217]	37	3[218]	114	24,5
Gesamtzahl Personen	740	4.359	4	5.103	

Probleme traten im Zusammenhang mit der Anerkennung der bestehenden und gleich- oder höherwertigen Überprüfungen aus dem Geheimschutz, der Luft- oder Atomsicherheit nur vereinzelt auf. Lediglich acht Sabotageschutzbeauftragte (fünf Fremdfirmen und drei Unternehmen mit eigener sicherheitsempfindlicher Stelle) wiesen auf Schwierigkeiten in dem Verfahren hin. Folgende Probleme wurden dabei genannt[219]:

- Fehlende gesetzliche Regelung zur Gleichwertigkeit, nur untergesetzlich empfohlen, deshalb teilweise nicht akzeptiert. Verschärft durch Unterschiede zwischen SÜG/LSÜG
- Das Unternehmen kannte die Überprüfung im Geheimschutz nicht und wollte sie daher erst nicht anerkennen.
- Luftsicherheitsüberprüfungen erfolgen durch den Auftraggeber direkt – es gibt keine zentrale Verwaltung im Unternehmen, sodass auch keine Bescheinigung ausgestellt werden kann. Zudem erhalten die Mitarbeiter selber auch keine Unterlagen, die für den Sabotageschutz verwendet werden können. Generell wäre eine Vereinheitlichung und Kooperation, d. h. Konsolidierung der Prozesse für Geheimschutz, Sabotageschutz, Atom- und Luftsicherheit wünschenswert.
- Der eine weiß nicht, was der andere tut. Die Überprüfungen werden gegenseitig nicht anerkannt oder nur durch mehrfache Telefonate und Versendung der kompletten Schriftverkehrvorgänge. Das bringt zusätzliche Arbeit
- Vorstrafen
- Dauer der Prüfung

[217] Drei Sabotageschutzbeauftragte gaben an, die Annerkennengsregelung genutzt zu haben, ohne jedoch konkrete Personenzahlen zu nennen.
[218] Zwei Sabotageschutz-Dienstleister gaben an, die Annerkennengsregelung genutzt zu haben, ohne jedoch konkrete Personenzahlen zu nennen.
[219] Ein Sabotageschutzbeauftragter bejahte das Vorliegen eines Problems, machte jedoch keine konkreten Angaben zur Art des Problems.

- Die Überprüfung im Sabotageschutz sollte in jedem Fall gemacht werden und die Personen im Geheimschutz abgemeldet werden => vollkommene Trennung der beiden Bereiche.

Die Sabotageschutzbeauftragten, die angaben, dass sie bislang noch keinen Gebrauch von der Anerkennensregelung gemacht haben, wurden darüber hinaus danach gefragt, was die Gründe hierfür waren. Etwa 86 Prozent der Befragten (303) gaben an, dass keine der Mitarbeiterinnen und keiner der Mitarbeiter, die an sicherheitsempfindlichen Stellen einzusetzen waren, eine gültige und gleich- oder höherwertige Überprüfung aus dem Geheimschutz, der Luft- oder Atomsicherheit hatte. Knapp 14 Prozent der Sabotageschutzbeauftragten (49) nannten hierfür andere Gründe. Am häufigsten wurde von den Befragten darauf hingewiesen, dass kein Bedarf für die Anwendung der Anerkennensregelung bestand bzw. diese keine Relevanz hat (29). Darüber hinaus gaben fünf Sabotageschutzbeauftragte an, dass sie die Anerkennensregelung gemäß § 2 Abs. 1 S. 5 SÜG nicht kannten. Weitere fünf Befragte machten keine Angaben zu den konkreten Gründen. Des Weiteren wurde die Nichtnutzung der Anerkennensregelung wie folgt begründet:

- Im Bereich Luftsicherheit wurden atomrechtliche Prüfungen nicht akzeptiert. Wir haben fünf Mitarbeiter im Bereich Sabotageschutz überprüft, ca. 12 im Bereich Luftsicherheit und 100 im Bereich atomrechtliche Prüfung.
- Sicherheitsüberprüfung KTA wurde nicht anerkannt.
- Überprüfungsfristen sind noch nicht abgelaufen.
- Vorschrift vom Kunden
- Wir haben immer Personal in ausreichendem Umfang
- War vor 2015
- Wurde vom Auftraggeber nicht anerkannt
- Arbeiten dauerten länger als die Dauer der Überprüfung
- Zeitablauf eingetreten
- Wir arbeiten nicht mehr für sicherheitsrelevante Firmen

Bewertung des mit der Umsetzung des vpS verbundenen Aufwands

Der Aufwand, der durch die Umsetzung des vpS in den Unternehmen entsteht, wurde von den Befragten weit überwiegend als nicht sehr hoch angesehen. So bewertete etwa die Hälfte der Sabotageschutzbeauftragten den Aufwand als sehr gering bzw. gering. Hingegen waren lediglich etwas mehr als sieben Prozent der Befragten der Meinung, dass der mit der Umsetzung des vpS verbundene Aufwand sehr hoch bzw. hoch ist. Knapp 34 Prozent der Sabotageschutzbeauftragten schätzten den Aufwand als mittel ein. Rund acht Prozent machten hierzu keine Angaben.

Tab. 26: Bewertung des mit der Umsetzung des vpS in den Unternehmen verbundenen Aufwands durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich

Aufwand Umsetzung vpS	FF (abs.)	in %	U. m. eig. seS (abs.)	in %	Sab-D. (abs.)	in %	Gesamt (abs.)	in %
Sehr gering	40	12,4	26	21,0	5	25,0	71	15,2
Gering	126	39,1	33	26,6	5	25,0	164	35,2
Mittel	105	32,6	47	37,9	6	30,0	158	33,9
Hoch	18	5,6	11	8,9	1	5,0	30	6,4
Sehr hoch	4	1,2	1	0,8	-	-	5	1,1
Keine Angabe	29	9,0	6	4,8	3	15,0	38	8,2
Gesamt	**322**	**100,0**	**124**	**100,0**	**20**	**100,0**	**466**	**100,0**

Bewertung der Zusammenarbeit mit dem BMWi als zuständige Stelle

Die Sabotageschutzbeauftragten wurden gefragt, wie sie insgesamt die Zusammenarbeit mit dem BMWi als zuständige Stelle bei der Durchführung der SÜ vpS bewerten. Hier zeigte sich ein eindeutiges Bild: Etwas mehr als 68 Prozent der Befragten bezeichnete die Zusammenarbeit mit dem BMWi als sehr gut bzw. gut. Knapp 24 Prozent der Sabotageschutzbeauftragten stuften die Kooperation als neutral ein. Lediglich knapp zwei Prozent bewerteten die Zusammenarbeit als schlecht. Sechs Prozent der Befragten machte hierzu keine Angaben.

Tab. 27: Bewertung der Zusammenarbeit mit dem BMWi durch die Sabotageschutzbeauftragten im nichtöffentlichen Bereich

Zusammenarbeit mit BMWi	FF (abs.)	in %	U. m. eig. seS (abs.)	in %	Sab-D. (abs.)	in %	Gesamt (abs.)	in %
Schlecht	6	1,9	3	2,4	-	-	9	1,9
Neutral	75	23,3	28	22,6	7	35,0	110	23,6
Gut	140	43,5	49	39,5	4	20,0	193	41,4
Sehr gut	79	24,5	41	33,1	6	30,0	126	27,0
Keine Angabe	22	6,8	3	2,4	3	15,0	28	6,0
Gesamt	**322**	**100,0**	**124**	**100,0**	**20**	**100,0**	**466**	**100,0**

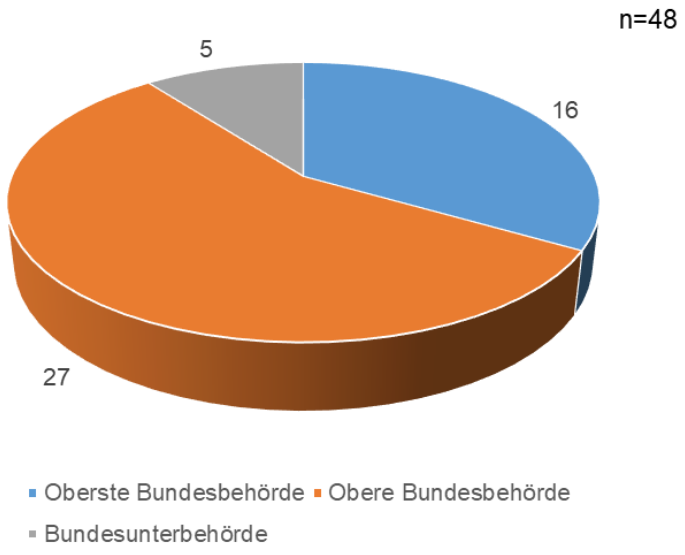
4.11.2.2.2. Öffentlicher Bereich

Um Erkenntnisse zu den Erfahrungen mit der Umsetzung des vorbeugenden personellen Sabotageschutzes (vpS) – insbesondere zur Nutzung der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) sowie zur Einschätzung des mit dem vpS verbundenen Aufwands – im öffentlichen Bereich gewinnen zu können, wurde im Mai/Juni 2017 eine online-gestützte Befragung der Sabotageschutzbeauftragten in der Bundesverwaltung (ohne den Geschäftsbereich des BMVg) durchgeführt. Hierzu wurde in enger Abstimmung mit dem für den vpS zuständigen Fachreferat im BMI ein Online-Fragebogen entwickelt.
Da es allerdings keinen Verteiler für alle Sabotageschutzbeauftragten in der Bundesverwaltung gab, wurde der Fragebogen-Link mit Passwort sowie ein Informationsschreiben vom BMI-Fachreferat per E-Mail an die obersten Bundesbehörden mit der Bitte weitergeleitet, diesen an die Sabotageschutzbeauftragten der Behörden in ihrem jeweiligen Geschäftsbereich zu verteilen. Insgesamt wurden 24 oberste Bundesbehörden sowie 28 Behörden im Geschäftsbereich des BMI direkt angeschrieben und aufgefordert, den Fragebogen auszufüllen bzw. weiterzuleiten.

Rücklauf

Insgesamt nahmen an der Befragung 48 Sabotageschutzbeauftragte teil. Da das BMI-Fachreferat keine Angaben dazu machen konnte, wie viele vom vpS betroffene Behörden es in den jeweiligen Geschäftsbereichen gibt, war es nicht möglich, eine Rücklaufquote für den gesamten öffentlichen Bereich zu ermitteln. Es konnte lediglich eine Aussage zur Rücklaufquote der obersten Bundesbehörden getroffen werden, von denen sich zwei Drittel an der Befragung beteiligten.
Hinsichtlich der Struktur des Rücklaufs lässt sich feststellen, dass der Großteil der Sabotageschutzbeauftragten in Bundesoberbehörden tätig war (27). Die zweitgrößte Gruppe stellten die Sabotageschutzbeauftragten der obersten Bundesbehörden dar (16), während nur wenige Sabotageschutzbeauftragte aus einer Bundesunterbehörde (5) stammten.

Abb. 15: Verteilung der Sabotageschutzbeauftragten nach Behördentypen



Der überwiegende Teil der Sabotageschutzbeauftragten war in der Laufbahngruppe des höheren Dienstes (28) eingruppiert. Ein weiteres Drittel (16) gehörte der Laufbahngruppe des

gehobenen Dienstes an, während ein nur kleiner Teil der Sabotageschutzbeauftragten (4) im mittleren Dienst eingruppiert war.

Identifikation einer sicherheitsempfindlichen Stelle in den Behörden

Knapp 48 Prozent der befragten Sabotageschutzbeauftragten (23) wiesen darauf hin, dass sie bislang noch nicht an der Identifikation oder Neufassung einer sicherheitsempfindlichen Stelle in ihrer Behörde beteiligt war. Etwas mehr als die Hälfte (25) gab an, in diesem Bereich bereits Erfahrungen gesammelt zu haben. Probleme bei der Identifikation der sicherheitsempfindlichen Stelle traten dabei in sechs Fällen (24 Prozent) auf, während dieser Prozess bei 19 Befragten (76 Prozent) problemlos abgelaufen war. Als Probleme, die bei der Identifikation oder Neufassung einer sicherheitsempfindlichen Stelle aufgetreten sind, wurden von den Befragten genannt:

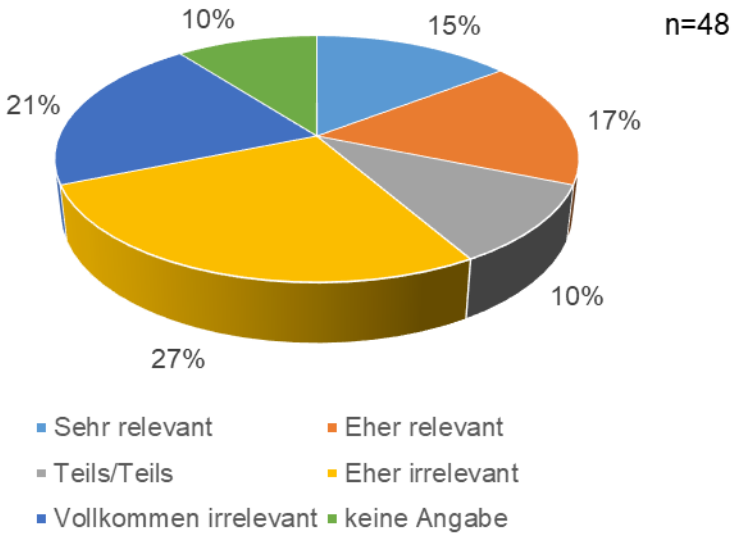
- Abgrenzung zu Maßnahmen des materiellen Geheimschutzes im IT-Bereich
- Definition einer sicherheitsempfindlichen Stelle im IT-Bereich aufgrund fehlender Einstufung als Sicherheitsbehörde nach SÜFV
- Die SÜFV ist in § 5b hinsichtlich der Beschreibung der lebenswichtigen Einrichtungen m. E. zu ungenau. Arbeitseinheiten, die den Betrieb der Informations- und Kommunikationstechnik sicherstellen und deren Ausfall die Tätigkeit der obersten Bundesbehörden unmittelbar erheblich beeinträchtigen könnte. Welcher Personenkreis könnte das sein (z. B alle Administratoren mit umfangreichen Berechtigungen, Zutrittsberechtigte RZ oder Andere?; nur wenige oder doch eher viele Überprüfungen?). In den Geschäftsbereichen gibt es hier unterschiedliche Auslegungen.
- Einheitliche Betrachtungsweise der verschiedenen Bereiche, die möglicherweise als sicherheitsrelevant einzustufen sind. Unterschiedliche Interpretation des Begriffs „sicherheitsrelevanter Bereich“
- Festlegung einer sicherheitsempfindlichen Stelle.
- Probleme bei der Festlegung, wer für die Identifizierung und Festlegung der Arbeitsplätze zuständig ist (auch wenn es klar geregelt ist). Akzeptanz bei betroffenen Organisationseinheiten und Mitarbeiterinnen und Mitarbeitern.

Nutzung und Bewertung der zeitlich erweiterten Ausnahmereglung (§ 9 Abs. 2 Nr. 2 SÜG)

Vom Großteil der befragten Sabotageschutzbeauftragten (34) wurde die Möglichkeit, bei Personen, die höchstens vier Wochen eine sicherheitsempfindliche Tätigkeit ausüben sollen und ständig durch eine überprüfte Person begleitet werden, von einer SÜ vpS abzusehen, bislang nicht genutzt. 14 Befragte machten seit 2016 bei insgesamt 1.402 Mitarbeiterinnen und Mitarbeitern von der Ausnahmeregelung Gebrauch. Hier reichte die Spannbreite von drei bis zu 900 Mitarbeiterinnen und Mitarbeitern.
Die Mitarbeiterinnen und Mitarbeiter, für die die Ausnahmereglung gemäß § 9 Abs. 2 Nr. 2 SÜG zur Anwendung kam, erledigten hauptsächlich kleinere Bau- und Reparaturarbeiten (9) sowie Wartungs- und Kontrolltätigkeiten (8). Darüber hinaus wurden sie auch für unregelmäßige Reinigungsarbeiten (6) und weitere Tätigkeiten (4) eingesetzt (z. B. Instandsetzungstätigkeiten, ehrenamtliche Einsatzaufgaben, weitere Tätigkeiten im Zusammenhang mit dem Gebäude).
Mit Blick auf die Ausweitung der Ausnahmeregelung von „in der Regel einem Tag“ auf nun „höchstens vier Wochen“ wurden die Sabotageschutzbeauftragten danach gefragt, wie sie

deren Relevanz für ihre Behörde bewerten. Rund 48 Prozent der Befragten wiesen darauf hin, dass die Ausweitung vollkommen bzw. eher irrelevant für ihre Behörde ist. Etwa drei von zehn Sabotageschutzbeauftragte schätzten die zeitlich erweiterte Ausnahmeregelung als sehr bzw. eher relevant ein, während fünf Befragte die Ausweitung teilweise relevant für ihre Behörde hielten. Fünf Sabotageschutzbeauftragte machten hierzu keine Angaben.

Abb. 16: Bewertung der zeitlich erweiterten Ausnahmereglung (§ 9 Abs. 2 Nr. 2 SÜG)



In diesem Zusammenhang wurde ebenfalls danach gefragt, ob die erweiterte Ausnahmereglung als ausreichend angesehen wird. Hier ergab sich ein eindeutiges Bild: 40 Sabotageschutzschutzbeauftragte hielten die zeitlich erweiterte Ausnahmeregelung für ausreichend, während acht Befragte der Auffassung waren, dass sie nicht ausreichend sei. Folgende Begründungen wurden hierfür genannt:

- Bei Bauarbeiten ist die Zeitdauer zu kurz bemessen.
- Das Wartungs- und Instandsetzungspersonal bedarf einer abgeschlossenen SÜ vpS. Die Ausnahme sollte eine Ausnahme bleiben. Deshalb ist ein Tag vollkommen ausreichend.
- Einsätze von externem Personal, Auszubildenden und Praktikanten sind oft auf drei bis vier Monate beschränkt.
- Mehr Flexibilität im Personaleinsatz erforderlich.
- Die Mitteilung des Ergebnisses einer SÜ vpS durch das BfV dauert länger (24 Wochen).
- Wegen der langen Bearbeitungsdauer im BfV sollte die Frist 12 Wochen betragen. Zudem betrifft der Sabotageschutz in meiner Behörde den ehrenamtlichen Bereich der Einsatzkräfte. Hier bedarf es oft besonderer Überzeugungsarbeit sich an der Sicherheitsüberprüfung zu beteiligen. Dies kann sehr zeitintensiv sein.
- Weil eine Begleitung niemals die notwendige Sicherheit gewährleistet. Daher sollte diese Ausnahmereglung in absoluten Notfällen zur Anwendung kommen.

Ein Sabotageschutzbeauftragter, der die zeitlich erweiterte Ausnahmeregelung für nicht ausreichend erachtete, machte hierzu keine weiteren Angaben.

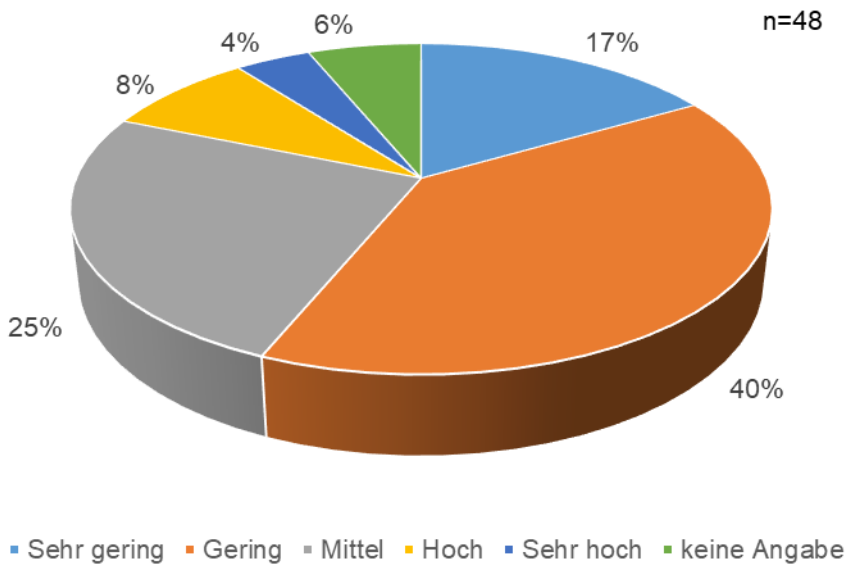
Nutzung der Anerkennensregelung nach § 2 Abs. 1 S. 5 SÜG

Des Weiteren wurden die Sabotageschutzbeauftragten dazu befragt, bei wie vielen Mitarbeiterinnen und Mitarbeitern sie seit 2015 von der SÜ vpS absehen konnten, weil bereits eine noch gültige gleich- oder höherwertige Überprüfung aus dem Geheimschutz, der Luft- oder der Atomsicherheit vorlag. In der einen Hälfte der Fälle (24) war dies nicht der Fall. In der anderen Hälfte (24) kam die Anerkennensregelung bei insgesamt 869 Personen zur Anwendung, wobei die Spannbreite von einem Mitarbeiter bis zu 320 Mitarbeiterinnen und Mitarbeitern reichte. Zwei Sabotageschutzbeauftragte machten hierzu keine weiteren Angaben.
In den Fällen, in denen von einer SÜ vpS abgesehen werden konnte, weil bereits eine noch gültige gleich- oder höherwertige Überprüfung aus dem Geheimschutz, der Luft- oder der Atomsicherheit vorlag, traten so gut wie keine Probleme bei der Anerkennung auf. Lediglich in einem Fall gab es Schwierigkeiten, da trotz des Verzichts auf eine SÜ vpS das BfV auf ausgefüllte Sicherheitserklärungen für den vpS bestanden hatte.

Bewertung des mit der Umsetzung des vpS verbundenen Aufwands

Der Aufwand, der im Zusammenhang mit der Umsetzung des vpS in den Behörden entsteht, wurde von etwa 56 Prozent der Sabotageschutzbeauftragten (27) als sehr gering bzw. gering eingeschätzt, während sechs Befragte diesen als sehr hoch bzw. hoch bewerteten. 12 Sabotageschutzbeauftragte stuften den mit der Umsetzung des vpS verbundenen Aufwand in ihrer Behörde als mittel ein. Drei Befragte machten hierzu keine Angaben.

Abb. 17: Bewertung des mit der Umsetzung des vpS verbundenen Aufwands durch die Sabotageschutzbeauftragten im öffentlichen Bereich

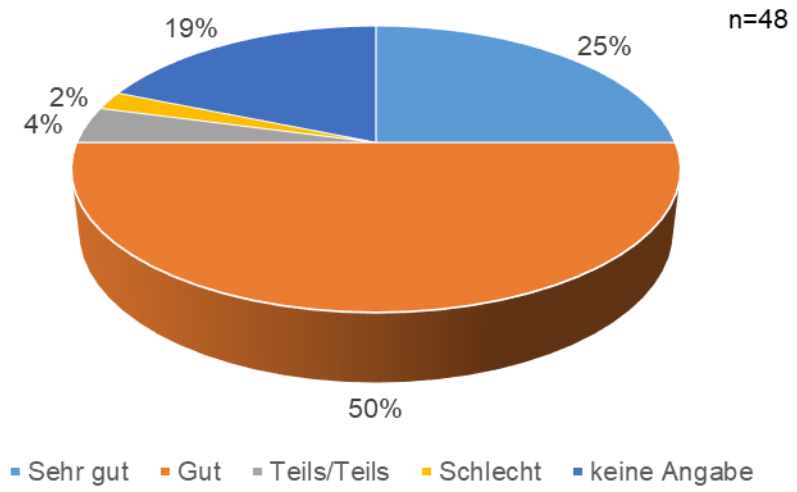


Bewertung der vom BfV übermittelten Informationen (Votum)

Im Rahmen der SÜ vpS übermittelt das BfV das Votum zu den überprüften Personen an die Sabotageschutzbeauftragten als zuständige Stelle. Auf dieser Grundlage entscheidet der Sabotageschutzbeauftragte der jeweiligen Behörde, ob eine Person an einer sicherheitsempfindlichen Stelle beschäftigt werden kann oder nicht. Die vom BfV übermittelten Informationen wurden von drei Viertel der Befragten (37) als sehr gut bzw. gut bewertet. Die Einschätzung von zwei Sabotageschutzbeauftragten war hingegen indifferent, während lediglich

ein Befragter die übermittelten Informationen als schlecht einstufte. Neun Sabotageschutzbeauftragte machten hierzu keine Angaben.

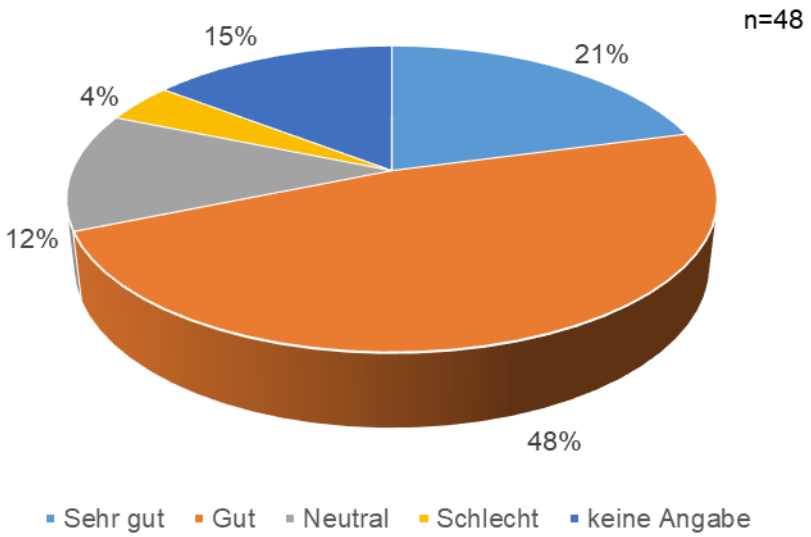
Abb. 18: Bewertung der vom BfV übermittelten Informationen (Votum) durch die Sabotageschutzbeauftragten im öffentlichen Bereich



Bewertung der Zusammenarbeit mit dem BfV als mitwirkende Behörde

Ein ähnlich gutes Bild ergibt sich bei der Bewertung der Zusammenarbeit mit dem BfV. Auch hier gab der Großteil der Befragten (33) an, dass die Zusammenarbeit sehr gut bzw. gut funktioniert. Sechs Befragte bewerteten die Kooperation mit der mitwirkenden Behörde als neutral. Lediglich zwei Sabotageschutzbeauftragte bezeichneten diese als schlecht, während sieben Befragte hierzu keine Angaben machten.

Abb. 19: Bewertung der Zusammenarbeit mit dem BfV durch die Sabotageschutzbeauftragten im öffentlichen Bereich



4.11.2.2.3. Militärischer Sicherheitsbereich

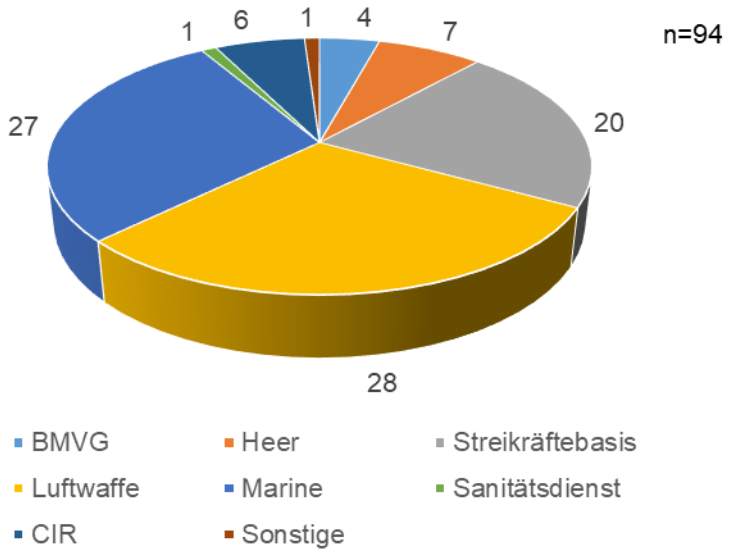
Um Erkenntnisse zu den Erfahrungen mit der Umsetzung des vpS – insbesondere zur Nutzung der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) sowie zur Einschätzung des mit dem vpS verbundenen Aufwands – im militärischen Sicherheitsbereich gewinnen zu können, wurde im August/September 2017 eine Befragung der SiBe, der GB sowie der HöSi durchgeführt. Hierzu wurden in enger Abstimmung mit dem für den vpS zuständigen Fachreferat im BMVg drei Fragebögen für o. g. Akteursgruppen, entwickelt. Insgesamt gibt es rund 1.500 SiBe im Geschäftsbereich des BMVg, wobei jedoch nur etwa 130 SiBe eine besonders sicherheitsempfindliche Stelle in ihrem Zuständigkeitsbereich hatten. Folglich erhielten vom BMVg nur diejenigen einen Fragebogen, in deren Zuständigkeitsbereich sich eine solche Stelle befand. Die Fragebögen sowie die Begleitschreiben wurden als Word-Formular über das BMVg an die entsprechenden Personen weitergeleitet. Nach Ablauf der Rückmeldefrist sammelte das zuständige Fachreferat die ausgefüllten Fragebögen wieder ein und übermittelte sie dann an das InGFA.

Rücklauf

Insgesamt nahmen an der Befragung 106 Personen aus dem militärischen Sicherheitsbereich teil (94 SiBe, neun HöSi[220] sowie drei GB[221].) Eine genaue Rücklaufquote lässt sich nur für die HöSi (100 Prozent) sowie für die GB (75 Prozent) angeben. Da das BMVg-Fachreferat keine exakte Zahl der SiBe mitteilen konnte, in deren Zuständigkeitsbereich sich eine besonders sicherheitsempfindliche Stelle befindet, konnte hier keine genaue Rücklaufquote ermittelt werden.
Da die drei Fragebögen z. T. unterschiedliche Fragen enthielten, erfolgt – sofern erforderlich – im Folgenden eine differenzierte Darstellung der Auswertungsergebnisse.
Zunächst ist festzuhalten, dass aus allen militärischen und aus fast allen zivilen Organisationsbereichen – mit Ausnahme der Personalverwaltung – SiBe an der Befragung teilgenommen haben. Die meisten Befragten waren in der Luftwaffe (28), der Marine (27) sowie der Streitkräftebasis (20) tätig. Aus dem Heer (8), dem Cyber- und Informationsraum (6), dem BMVg (4) sowie aus dem Sanitätsdienst und aus einer dem BMVg direkt unterstellten Dienststelle (je 1) stammten deutlich weniger SiBe.

[220] Insgesamt gibt es acht HöSi im Geschäftsbereich des BMVg. Neben den sechs militärischen Organisationsbereichen (Heer, Luftwaffe, Marine, Cyber- und Informationsraum, Kommando Streitkräftebasis, Zentraler Sanitätsdienst) und den drei zivilen Organisationsbereichen (Wehrtechnik, Verwaltung und Personal), wobei es für die Wehrtechnik und die Verwaltung einen gemeinsamen HöSi gibt, nahm noch ein Vertreter des Einsatzführungskommandos, für das es keinen offiziellen HöSi gibt, an der Befragung teil. Da dort vergleichbare Aufgaben wahrgenommen werden und ein Vertreter des Einsatzführungskommandos auch an den regelmäßigen Treffen der HöSi teilnimmt, wurden seine Angaben bei der Auswertung ebenfalls berücksichtigt.
[221] Das BAMAD nahm nicht an der Befragung teil. Allerdings sind SÜ vpS für das BAMAD nicht relevant, da die Mitarbeiterinnen und Mitarbeiter in der Regel über eine Ü3 (Geheimschutz) verfügen und somit keine SÜ vpS mehr erforderlich ist.

Abb. 20: Anzahl der SiBe nach Organisationsbereichen



Hinsichtlich der Eingruppierung der befragten SiBe, GB und HöSi ist festzuhalten, dass der überwiegende Teil der Befragten (66) im gehobenen Dienst tätig war. Hierbei handelte es sich vor allem um SiBe. Ähnlich verteilt sind die Eingruppierungen in den höheren (23) und mittleren Dienst (21), während nur ein Befragter im einfachen Dienst tätig war.

Tab. 28: Eingruppierung der für den vpS relevanten Akteure im militärischen Sicherheitsbereich

Laufbahn-/Entgeltgruppe	GB	SiBe	HöSi	Gesamt
Höherer Dienst (A 13-A 16 bzw. E 13-E 15)	2	12	9	23
Gehobener Dienst (A 9-A 13 bzw. E 9b bis E 12)	2	64	-	66
Mittlerer Dienst (A 6-A 9 bzw. E 5- E 9a)	1	20	-	21
Einfacher Dienst (A 2-A 6 bzw. E 1-E 4)	-	1	-	1
Gesamt	**5**[222]	**97**[223]	**9**	**111**

Identifikation sicherheitsempfindlicher Stellen in einer Dienststelle

53 Prozent der befragten SiBe (50) waren bislang noch nicht an der Identifizierung einer besonders sicherheitsempfindlichen Stelle in ihrer Dienststelle beteiligt. Hingegen gaben

[222] Ein GB gab drei Laufbahn-/Entgeltgruppen (höherer, gehobener und mittlerer Dienst) an, da sich die Aufgabe des GB auf mehrere Personen verteilt.
[223] Die Zahl ist höher als die oben angegebene Zahl von 95 SiBe, da in einem Fall zwei Laufbahn/ Entgeltgruppen (gehobener und mittlerer Dienst) und in einem anderen Fall drei Laufbahn-/Entgelt-gruppen (gehobener, mittlerer und einfacher Dienst) angegeben wurden.

knapp 46 Prozent (43) an, dass sie an einer solchen Identifikation mitgewirkt haben. Ein SiBe machte hierzu keine Angaben. Probleme traten dabei nur in wenigen Fällen (5) auf, während beim Großteil der Befragten (35) das Verfahren problemlos verlief. Drei SiBe machten hierzu keine Angaben.
Die Schwierigkeiten bei der Identifizierung einer besonders sicherheitsempfindlichen Stelle traten bei je zwei Dienststellen im Bereich der Streitkräftebasis und der der Marine sowie bei einer Dienststelle im Bereich der Luftwaffe auf. Hierbei handelte es sich um folgende Probleme:

- Finanzierung, Einhaltung langer Dienstwege, teilweise ungenaue bzw. widersprüchliche Vorschriften
- Es gibt Probleme in der Differenzierung zwischen dem Einsatz in Deutschland und dem Auslandseinsatz. In vielen Fällen ist innerhalb Deutschlands keine Sicherheitsüberprüfung im Bereich „Sabotageschutz“ vonnöten; bei Auslandseinsätzen z. B. auf Schiffen jedoch schon. Weiterhin ist in der Überprüfung gemäß Ü2/Ü3 VS der Sabotageschutz bereits inbegriffen, weshalb nicht weiter unterschieden wird zwischen dem tatsächlich notwendigen Einsatz im Bereich VS-Schutz UND/ bzw. Sabotageschutzbereich.
- Unterschiedliche Bewertungen, ob Schiffe und Boote SabSchutzDienststellen sind.
- Durch Umstrukturierungen wurden Räume der Liegenschaft umgenutzt. Somit mussten auch die Sperrzonen sowie Zutrittsregelungen und Absicherung (materiell und personell) neu betrachtet werden.
- Identifizierung einer Außenstelle bezüglich Bewachung

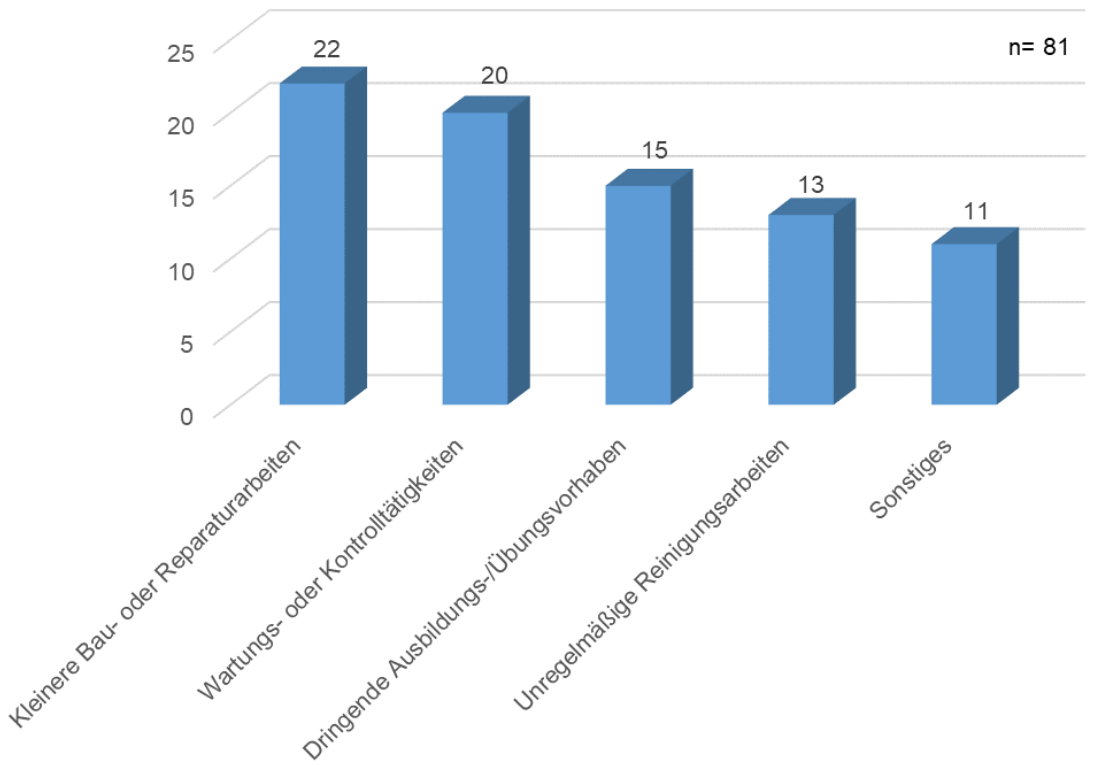
Sieben von neun HöSi gaben an, dass sie an der Identifizierung einer besonders sicherheitsempfindlichen Stelle in ihrem Bereich beteiligt gewesen sind, während dies bei zwei Befragten nicht der Fall war. Drei HöSi wiesen dabei auf Schwierigkeiten hin, die im Zusammenhang mit der Identifizierung aufgetreten sind. In vier Fällen verlief dieser Prozess problemlos. Bei den von den drei HöSi angesprochenen Problemen, die in den Bereichen Marine, Sanitätsdienst und Wehrtechnik/Verwaltung auftraten, handelte es sich um:

- *Erstens*: Es gab keine offiziellen verbindlichen Kriterien zur Festlegung der besonders sicherheitsempfindlichen Stellen. *Zweitens*: Es gab unterschiedliche Auffassungen innerhalb des BMVg in Bezug auf das entscheidende Kriterium (verteidigungswichtig gegenüber führungswichtig. *Drittens*: Die Feststellung einer besonders sicherheitsempfindlichen Stelle zieht aufgrund der Arbeitsüberlastung des BAMAD bei der Durchführung der Sicherheitsüberprüfungen eine erschwerte Besetzung der Stellen nach sich, deswegen wurde auch dieser Gesichtspunkt betrachtet, entgegen des Verständnisses des Sicherheitserfordernisses.
- Wenn man den Prozess zur Erarbeitung von klaren Vorstellungen als Schwierigkeiten oder Probleme bezeichnen will - Natürlich. Es gab einige Möglichkeiten der Interpretation und Auslegung die nach und nach geklärt wurden. Z. Z. ist die Problematik Einleitung von Ü 2 SabSchutz für hoheitliche Versender im Rahmen der Luftfrachtsicherheit aktuell.
- keine exakte Abgrenzung, Umsetzungsschwierigkeiten in der tatsächlichen Infrastruktur, unterschiedliche Bedürfnisse der verschiedenen OrgBereiche und dementsprechende Unklarheiten

Nutzung und Bewertung der zeitlich erweiterten Ausnahmereglung (§ 9 Abs. 2 Nr. 2 SÜG)

Mehr als zwei Drittel der befragten SiBe (63) machten von der zeitlich erweiterten Ausnahmeregelung gemäß § 9 Abs. 2 Nr. 2 SÜG keinen Gebrauch. Hingegen sah seit 2016 ein Drittel der Befragten (31) bei 511 Personen, die höchstens vier Wochen eine sicherheitsempfindlichen Tätigkeit ausüben und dabei ständig durch eine überprüfte Person begleitet werden, von einer SÜ vpS ab.
Hauptsächlich kam die zeitlich erweiterte Ausnahmeregelung zur Anwendung, damit die Mitarbeiterinnen und Mitarbeiter kleinere Bau- und Reparaturarbeiten (22) und Wartungs- und Kontrolltätigkeiten (20) erledigen konnten, ohne sicherheitsüberprüft werden zu müssen. Weitere Einsatzbereiche waren dringende Ausbildungs-/Übungsvorhaben (15), unregelmäßige Reinigungsarbeiten (13) sowie sonstige Tätigkeiten (11).

Abb. 21: Anwendungsbereiche der zeitlich erweiterten Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) im militärischen Sicherheitsbereich

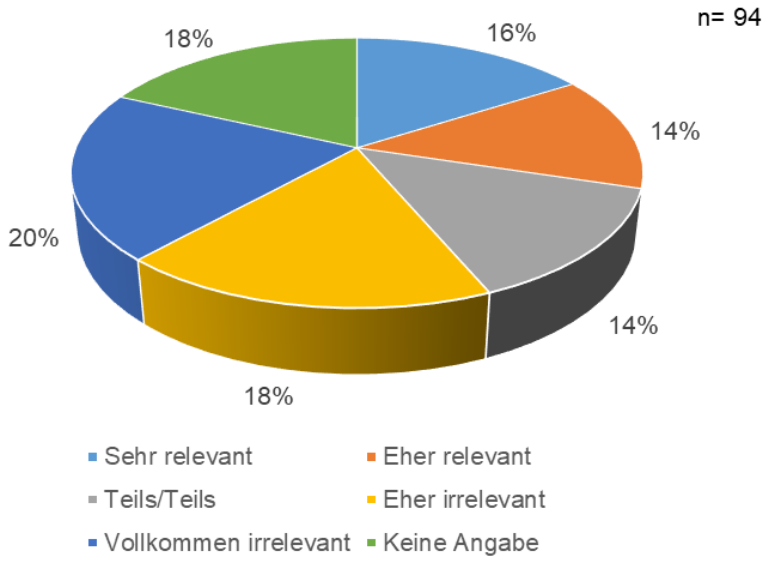


Bei den sonstigen Tätigkeiten handelte es sich um:

- Dienst an Bord; je nach Verwendungsreihe,
- Einsatz an Bord als Praktikant, Eignungsübende oder allgemeine Einschiffung,
- Grundsanierung eines Gebäudes,
- Neu zuversetzt,
- Praktika (4x),
- Regulärer Einsatz an Bord (Sabotageschutzbereich),
- Stabsdienstarbeiten,
- Wehrdisziplinaranwaltschaft.

Die Nicht-Anwendung der zeitlich erweiterten Ausnahmeregelung wurde von den befragten SiBe, die bislang keinen Gebrauch davon gemacht haben, damit begründet, dass in der jeweiligen Dienststelle grundsätzlich alle Personen, die an einer sicherheitsempfindlichen Stelle arbeiten (auch bei einem maximal vierwöchigen Einsatz), sicherheitsüberprüft werden (34) bzw. dass die Wartungs- und Kontrolltätigkeit durch Personal vorgenommen wird, das ohnehin dauerhaft an der sicherheitsempfindlichen Stelle beschäftigt ist (31). Darüber hinaus wurde als Grund genannt, dass die Bau- und Reparaturarbeiten länger als vier Wochen dauern (15). 23 SiBe gaben zudem sonstige Gründe an.
Die SiBe wurden auch danach gefragt, wie relevant die Ausweitung der Ausnahmeregelung in § 9 Abs. 2 Nr. 2 SÜG – von „in der Regel ein Tag“ auf nun höchstens vier Wochen“ – für ihre Dienststelle ist. Etwa 38 Prozent der Befragten (36) hielten die Ausweitung für vollkommen bzw. eher irrelevant. Hingegen stuften knapp 30 Prozent (28) sie als sehr bzw. eher relevant ein. Rund 14 Prozent der SiBe (13) hielten die Ausweitung für teilweise relevant, während 18 Prozent der SiBe (17) hierzu keine Angaben machten.

Abb. 22: Bewertung der zeitlich erweiterten Ausnahmereglung (§ 9 Abs. 2 Nr. 2 SÜG) durch die SiBe



Knapp 78 Prozent der befragten SiBe (73) gaben an, dass sie die Ausweitung der Ausnahmeregelung für ausreichend halten, während etwas mehr jeder fünfte Befragte der Meinung war, dass die Ausweitung nicht ausreichend ist.

Nutzung der Anerkennensregelung nach § 2 Abs. 1 S. 5 SÜG

Des Weiteren wurden die SiBe dazu befragt, bei wie vielen Mitarbeiterinnen und Mitarbeitern sie seit 2015 von der SÜ vpS absehen konnten, weil bereits eine noch gültige gleich- oder höherwertige Überprüfung aus dem Geheimschutz, der Luft- oder der Atomsicherheit vorlag. Bei etwas mehr als der Hälfte der Befragten (49) war dies nicht der Fall. Hingegen nutzten 44 Befragte seit 2015 die Anerkennensregelung bei insgesamt 5.229 Mitarbeiterinnen und Mitarbeitern. Dabei reichte die Spannbreite von einer Person bis zu 900 Personen. Ein SiBe machte zur konkreten Anzahl keine weiteren Angaben.
In den Fällen, in denen von einer SÜ vpS abgesehen werden konnte, weil bereits eine noch gültige gleich- oder höherwertige Überprüfung aus dem Geheimschutz, der Luft- oder der

Atomsicherheit vorlag, traten so gut wie keine Probleme bei der Anerkennung auf. Lediglich in einem Fall gab es Schwierigkeiten.
Zu den Gründen, warum ihre Dienststelle bislang noch keinen Gebrauch von der Anerkennensregelung gemacht hat, äußerten sich von den 49 SiBe, die dies angegeben hatten, lediglich acht. Fünf gaben an, dass keine der Mitarbeiterinnen und keiner der Mitarbeiter, die an einer sicherheitsempfindlichen Stelle einzusetzen waren, über eine gültige und gleich- oder höherwertige Überprüfung verfügte. Zwei Befragte nannten sonstige Gründe, wobei in einem Fall darauf hingewiesen wurde, dass ab 2015 grundsätzlich bei jeglicher sonstiger Sicherheitsüberprüfungshöhe eine SÜ vpS mit eingeleitet werden musste. Darüber hinaus begründete je ein SiBe, dass die Sicherheitsüberprüfung hier nicht gefordert ist bzw. für die Dienststelle nicht zutrifft. Ein Befragter machte keine Angabe zu den sonstigen Gründen.

Bewertung des mit der Umsetzung des vpS verbundenen Aufwands

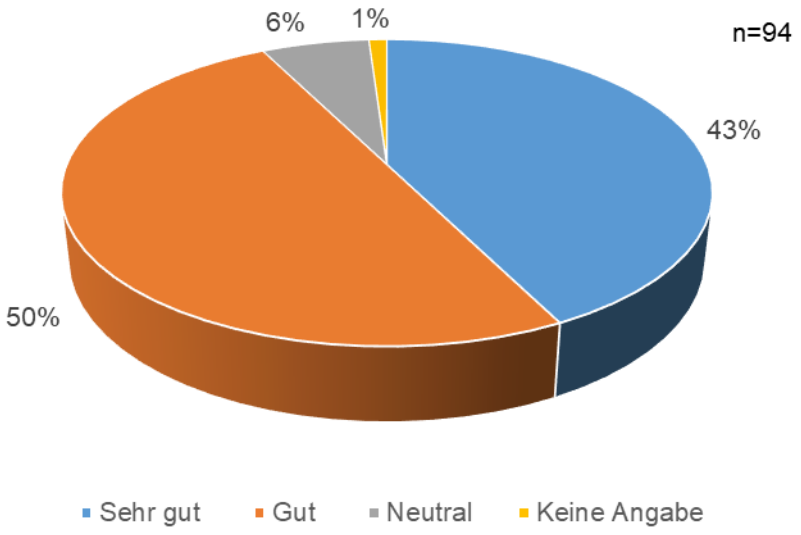
Der Aufwand, der im Zusammenhang mit der Umsetzung des vpS im militärischen Sicherheitsbereich entsteht, wurde von knapp 43 Prozent der befragten SiBe, GB und HöSi als sehr hoch bzw. hoch eingeschätzt, während lediglich 16 Prozent diesen als sehr gering bzw. gering einstuften. Knapp 30 Prozent der Befragten schätzten den mit der Umsetzung des vpS verbundenen Aufwand als mittel ein. Etwa 12 Prozent machten hierzu keine Angaben.

Tab. 29: Bewertung des mit der Umsetzung des vpS in den Dienststellen verbundenen Aufwands im militärischen Sicherheitsbereich

Bewertung Aufwand vpS	GB (abs.)	in %	SiBe (abs.)	in %	HöSi (abs.)	in %	Gesamt (abs.)	in %
Sehr gering	-	-	8	8,5	-	0,0	8	7,5
Gering	-	-	7	7,4	2	22,2	9	8,5
Mittel	1	33,3	28	29,8	3	33,3	32	30,2
Hoch	-	-	28	29,8	3	33,3	31	29,2
Sehr hoch	1	33,3	12	12,8	-	-	13	12,3
Keine Angabe	1	33,3	11	11,7	1	11,1	13	12,3
Gesamt	**3**	**100,0**	**94**	**100,0**	**9**	**100,0**	**106**	**100,0**

Die SiBe wurden zudem noch danach gefragt, wie sie die Zusammenarbeit mit dem BAMAD als mitwirkende Behörde bei der Durchführung von SÜ vpS bewerten. Hier zeigte sich ein eindeutiges Bild: Fast 93 Prozent der Befragten (87) bewerteten die Zusammenarbeit mit dem BAMAD als sehr bzw. eher gut. Sechs SiBe stuften die Zusammenarbeit mit der mitwirkenden Behörde als neutral ein. Ein Befragter machte hierzu keine Angaben.

Abb. 23: Bewertung der Zusammenarbeit mit dem BAMAD durch die SiBe



Auch die GB wurden gefragt, wie sie die Zusammenarbeit mit dem BAMAD als mitwirkende Behörde bei der Durchführung von SÜ vpS bewerten. Hier zeigte sich ein noch deutlicheres Bild als bei den SiBe. Alle drei GB, die an der Befragung teilgenommen haben, bewerteten die Zusammenarbeit mit dem BAMAD als sehr gut bzw. gut. Begründet wurde dies damit, dass die Zusammenarbeit vertrauensvoll sei und sich bewährt habe, ein intensiver Kontakt bzw. eine intensive Kooperation bestehe sowie die Bearbeiter immer für Erörterungen zur Verfügung stünden und umfänglich Auskunft gäben. Dieses positive Ergebnis spiegelte sich auch bei der Bewertung des vom BAMAD übermittelten Votums mit Blick auf die von den GB abschließend zu treffende Entscheidung wider. Auch hier bewerteten alle drei GB diese Informationen als sehr gut bzw. gut. Als Gründe hierfür wurden genannt, dass die Voten eine regelmäßige sachgerechte Grundlage für die abschließende Entscheidung böten, alle Informationen zur weiteren Bearbeitung vorhanden seien und es sich um qualitativ wertige Voten handele.

Des Weiteren wurden die GB danach gefragt, wie sie die Zusammenarbeit mit den SiBe bei der Durchführung von SÜ vpS bewerten. Auch hier ergibt sich ein ähnlich gutes Bild wie bei der Bewertung der Zusammenarbeit mit dem BAMAD. Zwei der drei GB bewerteten die Zusammenarbeit als sehr gut bzw. gut und begründeten dies damit, dass ein ständiger Kontakt (auch per Telefon) bestehe sowie die SiBe ansprechbar und auskunftsfähig seien. Ein GB schätzte die Zusammenarbeit als neutral ein, da die Intensität der Kooperation variiere, sich aber generell problemlos gestaltete.

Auch die HöSi wurden gefragt, wie sie insgesamt die Zusammenarbeit mit den ihnen unterstehenden SiBe bei der Durchführung von SÜ vpS bewerten. Sechs der neun Befragten bezeichneten die Zusammenarbeit mit den SiBe als sehr gut bzw. gut. Als Gründe für die sehr guten Bewertungen wurden genannt:

- Die entsprechenden Dienststellen sind nach den ministeriell (BMVg) vorgegebenen Kriterien seit Jahren identifiziert und handlungssicher in das Thema vpS eingewiesen, notwendige Infrastrukturmaßnamen sind zumeist abgeschlossen.
- Die SiBe sind dem HöSi fachlich unterstellt. Die Zusammenarbeit im Sachgebiet MilSichh ist gut und gedeihlich.
- nahezu täglicher Infoaustausch, i.d.R. pragmatische Lösungsansätze

Die guten Bewertungen wurden wie folgt begründet:

- Bei allen Beteiligten herrscht eine grundsätzliche Akzeptanz des Verfahrens.
- Gute Fachkenntnisse u. hohe Motivation aller Beteiligten vorhanden.
- Im Inland arbeite ich als HöSi nur mit zwei unterstellten SiBe zusammen. Dies erlaubt eine enge unmittelbare Abstimmung. In den Auslandseinsätzen der Bundeswehr spielt der vorbeugende personelle Sabotageschutz keine Rolle.

Ein Befragter gab eine neutrale Bewertung ab, da die Marine ohne Ausnahmegenehmigungen im Sabotageschutz ihren Auftrag nicht erfüllen könne, da Stellen nicht zu 100 Prozent besetzt seien und die Unterbesetzung zusätzlich durch nicht überprüftes Personal (bis zu zehn Prozent) verschärft werde. Während die SiBe der einen Flottille ständig im Kontakt mit dem HöSi Marine zwecks Erwirken von Ausnahmegenehmigungen gewesen sei, sei die andere Flottille nach dem Motto: „keine schlafenden Hunde wecken“ verfahren.
In zwei Fällen wurden hierzu keine Angaben gemacht. Ein Befragter begründet dies damit, dass jeder SiBe selbständig für die entsprechenden SÜ vpS zuständig sei und Fragen sich im Zusammenhang mit der SÜ vpS nicht ergäben. Ein weiterer HöSi nannte keinen konkreten Grund für seine Bewertung.

4.11.2.3. Gegenüberstellung der zentralen empirischen Ergebnisse für den nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich

Im Vergleich zur vorherigen Evaluation stellte die Einbeziehung der Sabotage- und Sicherheitsbeauftragten sowie der Geheimschutzbeauftragten und der HöSi (militärischer Sicherheitsbereich) eine Neuerung dar und ermöglichte tiefere Einblicke in die Anwendungspraxis der vpS-Regelungen im öffentlichen, nichtöffentlichen und militärischen (Sicherheits-)Bereich. Die drei Bereiche wiesen dabei nicht nur hinsichtlich der jeweiligen organisatorischen Ausgestaltung des vpS deutliche Unterschiede auf, sondern auch hinsichtlich der Nutzungshäufigkeit – gemessen an den pro Jahr eingeleiteten und abgeschlossenen SÜ vpS. Daher werden im Folgenden ausgewählte empirische Ergebnisse aus diesen drei Bereichen gegenübergestellt und erkennbare Unterschiede beschrieben.

Abgeschlossene und eingeleitete SÜ vpS

Personen, die im öffentlichen, nichtöffentlichen und militärischen (Sicherheits-)Bereich an einer (besonders) sicherheitsempfindlichen Stelle eingesetzt werden sollen, müssen sich hierfür einer SÜ vpS unterziehen. Im Untersuchungszeitraum wurden insgesamt 70.726 SÜ vpS eingeleitet und 75.545 SÜ vpS abgeschlossen. Etwa zwei Drittel der eingeleiteten sowie knapp 65 Prozent der abgeschlossenen SÜ vpS entfielen dabei auf den militärischen Sicherheitsbereich. Hingegen wurde das Instrument im nichtöffentlichen (14.736 eingeleitete und 14.272 abgeschlossene SÜ vpS) und im öffentlichen Bereich (10.317 eingeleitete und 10.768 abgeschlossene SÜ vpS) deutlich weniger genutzt.

Tab. 30: Eingeleitete und abgeschlossene SÜ vpS im nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich

	2015	2016	2017	Gesamt	Verände-rung 2017 ggü. 2015	Verände-rung in %
Abgeschlossene SÜ vpS						
militärischer Sicherheitsbereich	20.486	16.113	13.906	50.505	-6.580	-32,1 %
nichtöffentlicher Bereich	5.296	4.458	4.518	14.272	-778	-14,7 %
öffentlicher Bereich	3.303	4.014	3.451	10.768	148	4,5 %
Gesamt abgeschlossen	**29.085**	**24.585**	**21.875**	**75.545**	**-7.210**	**-24,8 %**
Eingeleitete SÜ vpS						
militärischer Sicherheitsbereich	16.589	15.644	13.440	45.673	-3.149	-19,0 %
nichtöffentlicher Bereich	5.544	4.185	5.007	14.736	-537	-9,7 %
öffentlicher Bereich	3.117	3.673	3.527	10.317	410	13,2 %
Gesamt eingeleitet	**25.250**	**23.502**	**21.974**	**70.726**	**-3.276**	**-13,0 %**

Anzumerken ist in diesem Zusammenhang, dass sowohl die Zahl der eingeleiteten als auch die Zahl der abgeschlossenen SÜ vpS seit 2015 – vor allem durch die Entwicklung im militärischen Sicherheitsbereich – insgesamt rückläufig ist. So ging die Zahl der abgeschlossenen SÜ vpS gegenüber dem Jahr 2015 um 7.210 zurück. Dies entspricht einem Rückgang von knapp 25 Prozent. Die Zahl der eingeleiteten SÜ vpS verringerte sich hingegen um 3.276, was einem Rückgang von dreizehn Prozent entspricht.

Identifikation (besonders) sicherheitsempfindlicher Stellen

Die Sabotageschutz- und Sicherheitsbeauftragten sowie die Höheren Offiziere Absicherung sind dafür verantwortlich, (besonders) sicherheitsempfindliche Stelle in ihrem jeweiligen Zuständigkeitsbereich zu identifizieren bzw. neu festzustellen. Knapp 47 Prozent der Befragten (137) gaben an, dass sie an diesem Prozess bereits mitgewirkt haben. Lediglich bei rund 15 Prozent (21) traten dabei Schwierigkeiten auf. Prozentual gesehen wiesen mehr mit der Identifikation von sicherheitsempfindlichen Stellen befasste Befragte aus dem öffentlichen Bereich (24 Prozent) auf Probleme hin als aus dem militärischen Sicherheitsbereich (16 Prozent) und dem nichtöffentlichen Bereich (rd. 11 Prozent).

Erweiterte Ausnahmeregelung gemäß § 9 Abs. 2 Nr. 2 SÜG

Die zeitlich erweiterte Ausnahmeregelung ermöglicht es den Sabotageschutz- und Sicherheitsbeauftragten Personen für höchstens vier Wochen (vorher: in der Regel höchstens einen

Tag) an einer sicherheitsempfindlichen Stelle tätig werden zu lassen, ohne dass sie vorher sicherheitsüberprüft worden sind, wenn sie von einer sicherheitsüberprüften Person ständig begleitet werden. Hiervor machten knapp 22 Prozent der Befragten überhaupt Gebrauch und sahen bei insgesamt 2.741 Mitarbeiterinnen und Mitarbeitern von einer SÜ vpS ab, wobei es z. T. deutliche Unterschiede zwischen den drei Bereichen gab. So hatte etwa jeder Dritte der befragten SiBe im militärischen Sicherheitsbereich diese Möglichkeit schon einmal genutzt, während dies im öffentlichen Bereich bei knapp 30 Prozent und im nichtöffentlichen Bereich bei knapp 19 Prozent der Sabotageschutzbeauftragten der Fall war. Der Großteil der Mitarbeiterinnen und Mitarbeiter, bei denen von der Durchführung einer SÜ vpS abgesehen wurde, wurde im öffentlichen (1.402) und im nichtöffentlichen (828) Bereich eingesetzt. Im militärischen Sicherheitsbereich wurde die Möglichkeit bei 511 Mitarbeiterinnen und Mitarbeitern genutzt.
Dies spiegelte sich auch in der Bewertung der Relevanz der zeitlich erweiterten Ausnahmeregelung durch die Befragten aus den drei Bereichen wider. Lediglich rund 20 Prozent der befragten Sabotageschutzbeauftragten und SiBe stuften sie als sehr bzw. eher relevant ein, während knapp 42 Prozent diese als vollkommen bzw. eher irrelevant einschätzten. Jedoch wurden auch hier Unterschiede zwischen dem öffentlichen und militärischen (Sicherheits-)Bereich einerseits und dem nichtöffentlichen Bereich andererseits deutlich.
Während rund 30 Prozent der Sabotageschutzbeauftragten bzw. SiBe im öffentlichen und militärischen (Sicherheits-)Bereich die zeitlich erweiterte Ausnahmereglung als sehr bzw. eher relevant bewerteten, waren es im nichtöffentlichen Bereich gerade einmal rund 17 Prozent. Gleichzeitig betrug der Anteil der Befragten im öffentlichen Bereich, der die Erweiterung als vollkommen bzw. eher irrelevant einstufte, knapp 48 Prozent, während es im nichtöffentlichen Bereich knapp 42 Prozent und im militärischen Sicherheitsbereich etwas mehr als 38 Prozent waren.

Tab. 31: Bewertung der Ausnahmeregelung (§ 9 Abs. 2 Nr. 2 SÜG) im nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich[224]

Bewertung § 9 Abs. 2 Nr. 2 SÜG	öB (abs.)	in %	nöB (abs.)	in %	mSB (abs.)	in %	Gesamt (abs.)	in %
Sehr relevant	7	14,6	35	7,5	15	16,0	57	9,4
Eher relevant	8	16,7	46	9,9	13	13,8	67	11,0
Teils/teils	5	10,4	68	14,6	13	13,8	86	14,1
Eher irrelevant	13	27,1	129	27,7	17	18,1	159	26,2
Vollkommen irrelevant	10	20,8	66	14,2	19	20,2	95	15,6
Keine Angabe	5	10,4	122	26,2	17	18,1	144	23,7
Gesamt	48	100,0	466	100,0	94	100,0	608	100,0

[224] **öB**=öffentlicher Bereich; **nöB**=nichtöffentlicher Bereich; **mSB**=militärischer Sicherheitsbereich

Hauptsächlich wurde die Ausnahmeregelung dazu genutzt, dass Mitarbeiterinnen und Mitarbeiter ohne SÜ vpS kleine Reparatur- und Bauarbeiten (knapp 34 Prozent) sowie Kontroll- und Wartungstätigkeiten (knapp 33 Prozent) an (besonders) sicherheitsempfindlichen Stellen ausüben konnten.[225] Der Großteil der Befragten (85 Prozent) zeigte sich mit der zeitlich erweiterten Ausnahmeregelung zufrieden. Lediglich knapp 15 Prozent der Befragten waren der Meinung, dass die Ausnahmeregelung nicht ausreichend sei, wobei der Anteil der Unzufriedenen im militärischen Sicherheitsbereich (etwas mehr als 21 Prozent) etwas höher ausfiel als im öffentlichen (knapp 17 Prozent) und nichtöffentlichen Bereich (etwas mehr als 13 Prozent).

Anerkennensregelung gemäß § 2 Abs. 1 S. 5 SÜG

Die Anerkennensregelung gemäß § 2 Abs. 1 S. 5 SÜG ermöglicht es den Sabotageschutz- und Sicherheitsbeauftragten von der Einleitung einer SÜ vpS bei Personen abzusehen, wenn bereits eine noch gültige gleich- oder höherwertige Überprüfung aus dem Geheimschutz, der Luft- oder der Atomsicherheit vorliegt. Knapp 70 Prozent der befragten Sabotageschutzbeauftragten und SiBe nutzten diese Möglichkeit bislang nicht, während 30 Prozent von der Anerkennensregelung Gebrauch machten. Dabei griffen die Hälfte der befragten Sabotageschutzbeauftragten im öffentlichen Bereich und knapp 47 Prozent der SiBe im militärischen Sicherheitsbereich auf diese Möglichkeit zurück, während dies lediglich knapp ein Viertel der Sabotageschutzbeauftragten im nichtöffentlichen Bereich taten. In den drei Bereichen kam diese Regelung bei 11.201 Personen zur Anwendung, wobei der überwiegende Teil der Personen im militärischen Sicherheitsbereich (5.229) und im nichtöffentlichen Bereich (5.103) aufgrund einer noch gültigen und gleich- oder höherwertigen SÜ nicht noch einmal überprüft werden musste. Im öffentlichen Bereich wurde diese Möglichkeit bei deutlich weniger Mitarbeiterinnen und Mitarbeitern (869) genutzt. Bei der Anerkennung traten kaum Probleme auf.

Tab. 32: Nutzung der Anerkennensregelung (§ 2 Abs. 1 S. 5 SÜG) im nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich

Anerkennung SÜ aufgrund bereits bestehender Überprüfung	öB (abs.)	in %	nöB (abs.)	in %	mSB (abs.)	in %	Gesamt (abs.)	in %
Nein	24	50,0	352	75,5	49	52,1	425	69,9
Ja	24	50,0	114	24,5	44	46,8	182	29,9
Keine Angabe	-	-	-	0,0	1	1,1	1	0,2
Gesamt	**48**	**100,0**	**466**	**100**	**94**	**100,0**	**608**	**100,0**
Anzahl MA	**869**	**7,8**	**5.103**	**45,6**	**5.229**	**46,7**	**11.201**	**-**

Lediglich knapp sechs Prozent der Befragten (10), welche die Anerkennensregelung genutzt haben, wiesen auf Schwierigkeiten hin, wobei der überwiegende Teil aus dem nichtöffentlichen

[225] Die Prozentwerte beziehen sich auf die Gesamtzahl der Nennungen. Da hier Mehrfachnennungen möglich waren, übersteigt die Anzahl der Nennungen die Gesamtzahl der Befragten, die hierzu Angaben gemacht haben.

Bereich (8) und jeweils ein Befragter aus dem öffentlichen Bereich und dem militärischen Sicherheitsbereich stammten.

Bewertung des mit der Umsetzung des vpS verbundenen Aufwands

Fast die Hälfte der Befragten (45 Prozent) bezeichnete den Aufwand als sehr gering bzw. gering, während lediglich knapp 14 Prozent diesen als sehr hoch bzw. hoch einschätzten. Allerdings zeigten sich auch hier z. T. deutliche Unterscheide zwischen den drei Bereichen. So ist der Anteil derer, die den Aufwand bei der Umsetzung des vpS als sehr hoch bzw. hoch bezeichneten, im militärischen Sicherheitsbereich mit mehr als 41 Prozent deutlich höher als im nichtöffentlichen (etwas mehr als sieben Prozent) und im öffentlichen (etwas mehr als 12 Prozent) Bereich. Hingegen war der Anteil derer, die den Aufwand als sehr gering bzw. gering einschätzten, im öffentlichen Bereich (mehr als 56 Prozent) und nichtöffentlichen Bereich (mehr als 50 Prozent) am höchsten, während er im militärischen Sicherheitsbereich mit 16 Prozent deutlich geringer ausfiel.

Tab. 33: Bewertung des mit der Umsetzung des vpS verbundenen Aufwands im nichtöffentlichen, öffentlichen und militärischen (Sicherheits-)Bereich

Bewertung Aufwand vpS	öB (abs.)	in %	nöB (abs.)	in %	msB (abs.)	in %	Gesamt (abs.)	in %
Sehr gering	8	16,7	71	15,2	8	7,5	87	14,0
Gering	19	39,6	164	35,2	9	8,5	192	31,0
Mittel	12	25,0	158	33,9	32	30,2	202	32,6
Hoch	4	8,3	30	6,4	31	29,2	65	10,5
Sehr hoch	2	4,2	5	1,1	13	12,3	20	3,2
Keine Angabe	3	6,3	38	8,2	13	12,3	54	8,7
Gesamt	**48**	**100,0**	**466**	**100,0**	**106**	**100,0**	**620**	**100,0**

4.11.3. Rechtswissenschaftliche Bewertung

Die erweiterte SÜ zum Zwecke des vorbeugenden personellen Sabotageschutzes stellt einen Eingriff in das Recht auf allgemeine Handlungsfreiheit, die informationelle Selbstbestimmung und in die Berufsausübungsfreiheit des Betroffenen dar.[226] Dem widerspricht es nicht, dass eine zwangsweise Durchsetzung der SÜ nicht zulässig ist, sondern vielmehr auf dem Entgegenkommen der betroffenen Personen beruht.[227] Entscheidet die zuständige Stelle,

[226] Vgl. BVerwG, Urteil vom 14.04.2011 – 3 C 24/10 – BeckRS 2011, 51678, Rn. 27 zum Eingriff in das Recht auf informationelle Selbstbestimmung durch § 7 LuftSiG. Zum Eingriff in die Berufsausübungsfreiheit durch ein Ermächtigungserfordernis zum Umgang mit Verschlusssachen OVG Münster, NJW 1985, 281 (283).
vgl. zum Ergebnis der Vereinbarkeit einer Zuverlässigkeitsüberprüfung mit Art. 12 Abs. 1 GG BVerfG, NVwZ 2009, 1429.

[227] Vgl. Vorbemerkungen Nr. 4 der Allgemeinen Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz – SÜG-Ausführungsvorschrift (SÜG-AVV) vom 15.2.2018 – ÖS II 5 – 54001/11#3, im Folgenden AllgVwV BMI.

dass ein Sicherheitsrisiko vorliegt oder liegt ein Verfahrenshindernis zum Abschluss einer solchen Überprüfung vor (etwa weil sich die betroffene Person einer Überprüfung verweigert), hat sie keine Chance, eine entsprechende Arbeitsstelle im sicherheitsempfindlichen Bereich zu finden.[228] Darüber hinaus existieren Berufe, die nur in sicherheitsempfindlichen Einrichtungen ausgeübt werden können.

Soweit es die erweiterte SÜ vpS im nichtöffentlichen Bereich anbetrifft, kann darüber hinaus das Grundrecht der Unternehmen aus Art. 12 Abs. 1 GG mit Blick auf die durch die SÜ vpS entstehenden Belastungen[229] sowie die Einschränkung der Möglichkeit zur freien Auswahl bzw. zum freien Einsatz der Beschäftigten berührt sein. Insgesamt sind zahlreiche Unternehmen betroffen und es werden jährlich mehrere tausend SÜ vpS im nichtöffentlichen Bereich durchgeführt. Zudem werden – wenn auch unzulässigerweise – teils SÜ in Ausschreibungen als Teilnahmevoraussetzung am Bieterwettbewerb gefordert.

An der Geeignetheit können prima facie durchaus Zweifel bestehen, haben in den Jahren 2015 bis 2017 doch gut 14.000 abgeschlossene SÜ vpS im nichtöffentlichen Bereich nur in einem Fall zu einer Feststellung eines Sicherheitsrisikos geführt. Doch dürfte durch die nicht zu unterschätzende abschreckende Wirkung der insoweit bestehende Einschätzungsspielraum des Gesetzgebers nicht verlassen worden sein, zumal das System sukzessive angepasst wird.[230] An diesem Ergebnis ändert auch die Möglichkeit der Tätigkeit an einer sicherheitsempfindlichen Stelle ohne SÜ von bis zu vier Wochen in ständiger Begleitung nichts, da das Sicherheitsniveau durch die Begleitung gewährleistet wird und zugleich der Überprüfungsaufwand reduziert wird. Schließlich kann die Möglichkeit künftiger Sabotageangriffe durch Innentäter nicht gänzlich ausgeschlossen werden.

Ein milderes, aber gleich wirksames Mittel als eine – ggf. (noch weiter) modifizierte – SÜ ist für Zwecke des vorbeugenden personellen Sabotageschutzes nicht erkennbar. Jede Erweiterung der SÜ vpS um eines Sicherheitsgewinns willen würde zugleich die Eingriffsintensität erhöhen. Umgekehrt gilt, dass jede Reduzierung oder gar Abschaffung des vorbeugenden personellen Sabotageschutzes das Schutzniveau reduzieren würde und damit weniger geeignet wäre.

Zum Maßstab für die Prüfung der Verhältnismäßigkeit im engeren Sinne ist zunächst darauf hinzuweisen, dass die SÜ vpS im Bereich der lebens- und verteidigungswichtigen Einrichtungen u. a. auf den Schutz von Leib und Leben großer Teile der Bevölkerung und damit auf hochrangige Rechtsgüter abzielt. Angesichts des hohen Gefährdungspotenzials können an die Überprüfung grundsätzlich hohe Anforderungen gestellt werden.[231] Gemessen an diesen Maßstäben hat die Analyse der durch die empirische Untersuchung erhobenen Daten keine Hinweise auf die Unverhältnismäßigkeit der Anwendung der erweiterten SÜ als solcher erbracht. Auch die im Verhältnis zur Zahl der durchgeführten erweiterten SÜ sehr kleine Zahl der Fälle mit ermitteltem Sicherheitsrisiko indiziert eine solche Unverhältnismäßigkeit nicht. Denn das Gewicht der beim vorbeugenden personellen Sabotageschutz in lebens- oder verteidigungswichtigen Einrichtungen oder dem militärischen Sicherheitsbereich in Rede stehenden Rechtsgüter gestattet aus verfassungsrechtlicher Perspektive eine lückenlose Überprüfung aller eine sicherheitsempfindliche Tätigkeit Ausübenden. Dabei ist mit Blick auf den Einzelfall

---

[228] Vgl. OVG Münster, NJW 1985, 281 (283) zur Ermächtigung zum Umgang mit Verschlusssachen im Bereich der Rüstungswirtschaft.

[229] Gut 40 Prozent gaben an, der mit dem vpS einhergehende Aufwand stelle sich als mittel, hoch oder sehr hoch dar.

[230] Vgl. zum Einschätzungsspielraum nur BVerfG, NVwZ 2009, 1429.

[231] Vgl. BVerfG, Beschluss vom 04.08.2009 – 1 BvR 1726/09 – NVwZ 2009, 1429; VGH München, Beschluss vom 14.07.2015 – 8 ZB 13.1666 – NVwZ-RR 2015, 933, Rn. 8 zu § 7 LuftSiG. Zum vorbeugenden personellen Sabotageschutz liegt keine entsprechende Rechtsprechung vor.

zu berücksichtigen, dass die Eingriffsintensität nicht besonders hoch ist. Denn die bei der SÜ vpS erhobenen Daten sind weder dem Kernbereich privater Lebensgestaltung zuzurechnen, da insbesondere keine Referenzpersonen befragt werden, noch werden die Partner einbezogen. Damit bestehen keine rechtswissenschaftlichen Bedenken bzgl. der Anwendungspraxis des vorbeugenden personellen Sabotageschutzes. Allein die dargestellten Probleme der in Ausschreibungen definierten Teilnahmevoraussetzungen einer vorhandenen SÜ vpS sowie die teils fehlende Anerkennung der Ü2 vpS im öffentlichen Bereich auf Landesebene mit der Folge von Doppelüberprüfungen[232] sollte der Gesetzgeber adressieren.

[232] Vgl. die Angaben des BMI unter Kapitel 4.11.2.1.1.

5. Probleme der Anwendungspraxis im Spiegel der Konsistenz nachrichtendienstlicher Befugnisse

Die Nachrichtendienste wiesen im Rahmen der Interviews immer wieder auf praktische Probleme hin, die auf inkonsistente Regelungen im System der besonderen Auskunftsverlangen sowie des IMSI-Catchers und dort auf teils überhöhte Anforderungen auf tatbestandlicher Ebene, aber auch auf die Pflichten zur Mitteilung zurückzuführen seien. Diese in der Regel als Optimierungsvorschläge formulierten Hinweise sind bei den jeweiligen Normen dokumentiert. Im Folgenden werden sie exemplarisch für das BVerfSchG einer systematischen Betrachtung unterworfen.

5.1. Zentrale Ergebnisse

Bei Betrachtung der besonderen Auskunftsverlangen fällt auf, dass in zahlreichen Fällen, in denen weder ein Eingriff in Art. 10 GG noch ein erheblicher Eingriff in das Persönlichkeitsrecht vorliegt, dennoch das G 10-Verfahren vorgesehen wird. Zudem stellen sich die Anforderungen in Bezug auf Schutzgut, Gefahrengrad und Verfahren teils wenig konsistent dar. So werden einerseits vergleichbare Anforderungen an Maßnahmen gestellt, die in ihrer Eingriffsintensität weit auseinanderliegen (augenfällig bei vorbereitenden Maßnahmen zu Folgemaßnahmen: Kontostammdaten zu Kontoinhalten; IMSI-Catcher zu G 10-Maßnahmen). Andererseits fallen die tatbestandlichen Voraussetzungen teils erheblich auseinander, obschon eine vergleichbare Eingriffsintensität vorliegt (TK-Bestandsdaten wie auch Kontostammdaten [jeweils G 10-Verfahren] zu Teledienst-Bestandsdaten [keine besonderen Verfahrensanforderungen]). Schließlich können andere Behörden die gleichen Maßnahmen unter teils (erheblich) geringeren Kautelen durchführen (Kontostammdatenerhebung sehen bei Nachrichtendiensten das G 10-Verfahren, bei Polizei [auch des Bundes], Sozialbehörden etc. dagegen kein besonderes Verfahren vor).
Auch die Mitteilungspflicht ist widersprüchlich geregelt, wenn bei schwerwiegenderen Eingriffen ein endgültiges Absehen von der Mitteilung möglich ist, bei leichteren Eingriffen dagegen nicht (G 10-Maßnahmen und Maßnahmen nach § 8a Abs. 2 S. 1 Nr. 4 und 5 gegenüber solchen nach § 8a Abs. 2 S. 1 Nr. 1 und 2 sowie Abs. 2a BVerfSchG).

5.2. Verfassungsrechtlicher und sicherheitspolitischer Rahmen

Der Gesetzgeber hat verfassungsrechtlich gesehen einen äußerst großen Ermessensspielraum, „überobligatorischen Grundrechtsschutz“ durch hohe tatbestandliche Anforderungen auch an wenig invasive Maßnahmen zu gewährleisten.[233] Eine Grenze könnte sich dort ergeben, wo Maßnahmen praktisch undurchführbar werden und damit der gesetzliche Auftrag des Nachrichtendienstes in Frage gestellt würde. Sollte der Gesetzgeber jedoch Befugnisse vorsehen und eine effektive nachrichtendienstliche Arbeit anstreben, so sollte er die Befugnisse möglichst konsistent fassen. Folgende Prinzipien erscheinen sinnvoll:

- Die tatbestandlichen Anforderungen sollten (in materieller wie formeller Hinsicht) mit der Eingriffsintensität steigen und umgekehrt. Dies würde zudem der Logik des Verhältnismäßigkeitsprinzips entsprechen.

[233] Der Gesetzgeber könnte auf das Einräumen der in Rede stehenden Befugnisse sogar gänzlich verzichten.

– Für Maßnahmen mit vergleichbarer Eingriffsintensität sollten vergleichbare Anforderungen formuliert werden, jedenfalls sollten leichtere Maßnahmen nicht an höhere Anforderungen gekoppelt werden.

Bei der Betrachtung der tatbestandlichen Anforderungen an die besonderen Auskunftsverlangen und den IMSI-Catcher ist zu berücksichtigen, dass nachrichtendienstliche Tätigkeit in Wesen und Zweck Vorfeldaufklärung ist. Zahlreiche Maßnahmen dienen lediglich der Generierung von Vorinformationen („Puzzlestücke"), deren Relevanz im Vorhinein regelmäßig kaum abgeschätzt werden kann und die sich im Nachhinein nicht selten für sich als wenig relevant darstellt. Durch hohe Anforderungen gerade in formeller Hinsicht – etwa durch Anordnung des G 10-Verfahrens – wird ein außerordentlicher Ressourceneinsatz bei der Informationserlangung abverlangt. Dieser Aufwand kann nach Aussage der Nachrichtendienste immer wieder nicht geleistet werden, obschon der Tatbestand im Übrigen erfüllt ist. Entgegen dem Charakter der Vorfeldaufklärung haben sich zudem die tatbestandlichen Anforderungen, gerade was die Tatsachenlage betrifft, zunehmend denen polizeilicher Behörden angenähert, obgleich bei letzteren aus der Natur der Gefahrenabwehr heraus die Sachverhalte klarer auf der Hand liegen und sich in derselben Behörde zu robusten Maßnahmen über die Informationsgewinnung hinaus gegen den Betroffenen verdichten können. Teil einer konsistenten Fassung der nachrichtendienstlichen Befugnisse und gerade auch der besonderen Auskunftsverlangen ist eine Regelung der Voraussetzungen entsprechend der Grundrechtsrelevanz, zumal die Anordnung des G 10-Verfahrens auch bei wenig invasiven Maßnahmen nicht nur Ressourcen der Nachrichtendienste, sondern auch der G 10-Kommission binden.

5.3. Überlegungen zu den einzelnen Befugnissen

Im Folgenden werden die einzelnen Befugnisse im Kontext betrachtet.

5.3.1. § 8 Abs. 1 BVerfSchG (Bestandsdaten Teledienste)

Es erscheint systemwidrig, dass die materiellen Anforderungen bei der Abfrage von Bestandsdaten bei Telediensteanbietern höher sind, als solche bei der Abfrage von Bestandsdaten bei Telekommunikationsunternehmen (TK), da die Eingriffstiefe sich als vergleichbar darstellt. Im TK-Bereich genügt nach § 8d BVerfSchG i. V. m. § 113 TKG ein Bezug zur Aufgabenerfüllung, § 8a Abs. 1 BVerfSchG verlangt demgegenüber tatsächliche Anhaltspunkte für eine schwerwiegende Gefahr für ein Schutzgut.
Zudem wurde inkonsequenterweise – und mit Blick auf die Grundrechtsrelevanz unnötigerweise – (nur) für die Abfrage von Bestandsdaten bei Telediensteanbietern, nicht jedoch für die Abfrage von Bestandsdaten bei TK-Unternehmen eine Mitteilungspflicht vorgesehen.
Mit Blick auf das Verhältnis zu den teils deutlich eingriffsintensiveren Maßnahmen nach § 8a Abs. 2 BVerfSchG und nach dem G 10 erscheinen die tatbestandlichen Anforderungen insgesamt hoch und die Mitteilungspflicht nicht zwingend geboten. Gerade die Notwendigkeit, dass die G 10-Kommission über eine endgültige Nichtmitteilung entscheiden muss, verwischt den erheblichen Unterschied in der Freiheitsrelevanz zu echten G 10-Maßnahmen[234].

[234] Zudem würde die G 10-Kommission entlastet.

5.3.2. § 8a Abs. 2 S. 1 Nr. 1 BVerfSchG (Flugdaten)

Bei Flugdaten zeigen sich auf tatbestandlicher Ebene wie auch bei den Mitteilungspflichten Inkonsistenzen. Es werden hohe materielle Anforderungen und das G 10-Verfahren angeordnet, obschon kein Eingriff in Art. 10 GG vorliegt und eine eher geringe Eingriffsintensität besteht.[235]

Mit Blick auf die Beteiligung der G 10-Kommission soll an dieser Stelle auch dem teils pauschal vorgebrachten Argument entgegengetreten werden, dass praktisch jeder heimliche Eingriff einer unabhängigen verfahrensmäßigen Kontrolle bedürfe. Zweifelsohne ist der Rechtsschutz bei heimlichen Maßnahmen deutlich erschwert, doch erfordert dies nicht per se eine präventive unabhängige Kontrolle. Vielmehr hat das BVerfG insoweit dargelegt, dass „eingriffsintensive[n] Überwachungs- und Ermittlungsmaßnahmen, bei denen damit zu rechnen ist, dass sie auch höchstprivate Informationen erfassen, und gegenüber den Betroffenen heimlich durchgeführt werden, (…) grundsätzlich einer vorherigen Kontrolle durch eine unabhängige Stelle [bedürfen]“[236]; hier ist auf die Kumulation auf der Eingriffsseite hinzuweisen (höchstprivat und heimlich), die bei Flugdaten gerade mangels besonderer Privatheit nicht gegeben ist. Im Übrigen müssten sonst alle geheimen Maßnahmen der Sicherheitsbehörden unter eine präventive unabhängige Kontrolle gestellt werden. Schließlich stellen sich die Anforderungen als vergleichbar mit denen von G 10-Maßnahmen dar, obschon die Flugdatenabfrage eine deutlich geringe Freiheitsbeschränkung mit sich bringt. Hier erschiene eine Anordnung durch das Ministerium als verfahrensrechtliche Absicherung mittlerer Reichweite (gegenüber Anordnung durch Sachbearbeiter bzw. G 10-Kommission) naheliegend, um der freiheitsrelevanten Stufung gerecht zu werden.

Bezüglich der Mitteilungspflicht ist bei Flugdaten[237] systemwidrig keine endgültige Nichtmitteilung nach § 12 Abs. 1 S. 5 G 10 möglich, obschon dies bei (grundrechtsrelevanteren) Maßnahmen nach dem G 10, aber auch nach § 8a Abs. 2 S. 1 Nr. 4 und 5 BVerfSchG vorgesehen ist. Dies lässt sich aus Konsistenzperspektive nicht rechtfertigen. Auch das im Wolff-Gutachten vorgebrachte Argument, dass ansonsten an keiner Stelle eine unabhängige Stelle beteiligt wäre[238], greift nicht mehr, da erstens derzeit jedenfalls für die Maßnahmen nach § 8a Abs. 2 S. 1 Nr. 1 und 2 BVerfSchG die G 10-Kommission beteiligt ist und zweitens in jedem Fall die G 10-Kommission über die endgültige Nichtmitteilung zu entscheiden hätte. Besonders virulent wird der Widerspruch dort, wo durch die Mitteilung der Flugdatenerhebung der Betroffene indirekt von einer parallel gegen ihn durchgeführten G 10-Maßnahme erfahren würde. Auch wenn er insoweit keine Details erfahren würde, wäre der Sinn der endgültigen Nichtmitteilung der G 10-Maßnahme unterminiert.

Hauptargument für die Verschärfung der tatbestandlichen Anforderungen bei den Flugdaten war 2011 die Herstellung einer inneren Konsistenz durch Angleichung an die Anforderungen des IMSI-Catchers[239] (§ 9 Abs. 4 BVerfSchG). Dies vermag für sich nicht zu überzeugen. Zum einen wäre eine Angleichung „nach unten“ ebenso möglich gewesen (da auch der IMSI-

---

[235] So jedenfalls Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011, S. 56, das im Vorfeld der Novellierung 2011 eingeholt wurde.

[236] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, Rn 117.

[237] Wie auch bei Konto-Maßnahmen nach Nr. 2 und Abs. 2a.

[238] Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011,S. 86.

[239] Wolff, Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011,S. 57.

Catcher keinen Eingriff in Art. 10 GG darstellt[240] und auch sonstige Gründe nicht zwingend für die Beteiligung der G 10-Kommission sprechen, siehe auch unten zu IMSI-Catcher). Zum anderen sind die Stoßrichtungen von IMSI-Catcher und Flugdatenauskunft durchaus so unterschiedlich, dass eine unterschiedliche Regelung keinesfalls einen Systembruch darstellen würde: Bei ersterem ist eine (kurzzeitige) Ortung möglich, bei letzterem nur Flugreisewege. Ebenso wenig überzeugt das Argument, dass alle besonderen Auskunftsverlangen gleich zu behandeln seien, da der Gesetzgeber sie als solche zu einer Gruppe zusammengefasst habe[241]. Denn es kommt für die Bestimmung verfassungsrechtlich gebotener Kautelen auf die Eingriffsintensität an, nicht auf eine etwaige Gruppierung durch den Gesetzgeber.[242]

5.3.3. § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG (Finanztransferdaten)

Die tatbestandlichen Anforderungen erscheinen angesichts der recht tiefen Eingriffe in die informationelle Selbstbestimmung und in das allgemeine Persönlichkeitsrecht durchaus systemgerecht, wenn auch das G 10-Verfahren mangels Eingriffs in Art. 10 GG verfassungsrechtlich nicht geboten ist. Es fällt auf, dass die administrative Financial Intelligence Unit (FIU) Finanztransferdaten (und Kontostammdaten) nach dem neuen GwG deutlich leichter, ohne ein besonderes Verfahren, abrufen kann.
Zudem ergibt sich auch hier ein Bruch bei der fehlenden Möglichkeit der endgültigen Nichtmitteilung bei Finanztransferdaten, obschon bei (grundrechtsrelevanteren) Maßnahmen nach dem G 10, aber auch nach § 8a Abs. 2 S. 1 Nr. 4 und 5 BVerfSchG eine endgültige Nichtmitteilung möglich ist. Dies lässt sich aus Konsistenzperspektive nicht rechtfertigen. Ebenso wenig überzeugt auch hier das Argument, dass alle besonderen Auskunftsverlangen gleich zu behandeln seien, da der Gesetzgeber sie als solche zu einer Gruppe zusammengefasst habe. Denn es kommt für die Bestimmung verfassungsrechtlich gebotener Kautelen auf die Eingriffsintensität an, nicht auf eine etwaige Gruppierung durch den Gesetzgeber.

5.3.4. § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG (TK-Verkehrsdaten) sowie § 8a Abs. 2 S. 1 Nr. 5 BVerfSchG (Nutzungsdaten Telediensteanbieter)

Sowohl die Abfrage von TK-Verkehrsdaten als auch für die Abfrage von Nutzungsdaten bei Telediensteanbietern greifen durch die Möglichkeit der umfangreichen Beleuchtung von Kommunikationsbeziehungen so erheblichen in das allgemeine Persönlichkeitsrecht ein, dass die tatbestandlichen Anforderungen sich als durchaus systemgerecht darstellen.

5.3.5. § 8a Abs. 2a BVerfSchG (Kontostammdaten)

Die Kontostammdatenabfrage stellt einen Eingriff von sehr geringem Gewicht in das allgemeine Persönlichkeitsrecht dar, da lediglich mitgeteilt wird, ob ein Konto besteht und falls dem so ist, die Kontoidentifikationsmerkmale. Insofern ist festzustellen, dass die Tatsache, dass die Kontostammdatenabfrage regelmäßig der Vorbereitung einer Finanztransferdatenabfrage dient, den Eingriff nicht vertieft. Vielmehr erschöpft sich die – durchaus erhebliche – Freiheitsbeschränkung in der dann erfolgenden konkreten Finanztransferdatenabfrage, weshalb diese entsprechenden Kautelen zu unterwerfen ist. Sollte der Betroffene etwa kein Konto in Deutschland haben, so bliebe es bei der wenig invasiven Kontostammdatenabfrage und ein

[240] Vgl. dazu auch die Novellierung des BayVSG, das nunmehr ausdrücklich kein G-10 Verfahren mehr vorsieht; vgl. die Begründung, LT-Drs. 17/10014, S. 33.
[241] In die Richtung Wolff, S. 41 unter dem Stichwort innergesetzliche Symmetrie.
[242] Zumal dieser insoweit wenig konsequent war, da der Sache nach auch die TK-Bestandsdaten nach § 8d BVerfSchG den besonderen Auskunftsverlangen (in Abgrenzung zu § 8 BVerfSchG) zuzuordnen wäre.

G 10-Verfahren würde „über das Ziel hinausschießen“. Im Vergleich zur Finanztransferdatenabfrage werden dieselben Anforderungen gestellt, obschon die Eingriffstiefe erheblich abweicht. Auch mit Blick auf TK-Bestandsdatenabfragen nach § 8d BVerfSchG zeigt sich eine fehlende Konsistenz, da die Abfrage von TK-Bestandsdaten mindestens ebenso grundrechtsintensiv wie die Abfrage von Kontostammdaten ist und dennoch die Anforderungen bzgl. Tatbestand und Mitteilungspflicht erheblich auseinanderfallen. Im Übrigen gelten die Ausführungen zu den Flugdaten entsprechend.
Schließlich fällt auf, dass andere Behörden deutlich leichter Kontostammdaten abrufen können:

- Sozialverwaltung (§ 93 Abs. 8 S. 1 Nr. 1 AO)
  - Materiell geringe Anforderungen: Erforderlichkeit und vorheriges Auskunftsersuchen beim Betroffenen fehlgeschlagen oder aussichtslos
  - Formell ist kein besonderes Verfahren vorgesehen
- Polizeivollzugsbehörden des Bundes und der Länder (§ 93 Abs. 8 S. 1 Nr. 2 AO)
  - Materiell nicht unerhebliche Anforderungen: Erforderlich für Abwehr einer erheblichen Gefahr für öffentliche Sicherheit
  - Formell kein besonderes Verfahren vorgesehen
- Finanzbehörden (§ 93 Abs. 8 AO)
  - Materiell eher geringe Anforderungen: wenn erforderlich für Besteuerung
  - Formell kein besonderes Verfahren vorgesehen
- Strafverfolgungsbehörden (§ 24c Abs. 3 S. 1 Nr. 2 KWG)
  - Materiell geringe Anforderungen: „soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist“
  - Formell kein besonderes Verfahren vorgesehen, lediglich Protokollierungspflicht (Abs. 4)
- Gerichtsvollzieher/Zwangsvollstreckung (§ 802l Abs. 1 S. 1 Nr. 2 ZPO)
  - Materiell geringe Anforderungen: Wenn Schuldner Abgabe zur Vermögensauskunft nicht nachkommt oder eine Vollstreckung in die darin angegebenen Vermögengegenstände für vollständige Befriedigung voraussichtlich nicht zu erwarten ist
  - Formell kaum Anforderungen, lediglich gewisse Protokollierungs- und Löschungspflichten in Abs. 2-5

5.3.6. § 9 Abs. 4 BVerfSchG (IMSI-Catcher)

Es fällt auf, dass bei der Anordnung des IMSI-Catchers nahezu identische Anforderungen wie bei G 10-Maßnahmen bestehen. Dies stellt sich aus folgenden Gründen als wenig konsistent dar. Zum einen wird regelmäßig nur die Telefonnummer des Betroffenen identifiziert. Diese weist für sich keinen besonderen Persönlichkeitsbezug auf und ein solcher kann ohne weitere Maßnahmen auch nicht hergestellt werden. Zum anderen bietet auch die Lokalisierungsfunktion nach Auskunft des BMI aus technischen Gründen keine Möglichkeit, Bewegungsprofile zu erstellen, da zur Durchführung der Messung der Standort vorab bekannt sein muss. Die Lokalisierungsfunktion bezieht sich mithin lediglich auf kleinräumige Gegebenheiten, wie der Feststellung eines konkreten Aufenthaltsortes.
Der Einsatz des IMSI-Catchers dient damit letztlich der Vorbereitung einer G 10-Maßnahme oder einer Abfrage von TK-Verbindungsdaten. Diese unterliegen ihrerseits den strengen Anforderungen des G 10 bzw. einem G 10-analogen Verfahren. Sollte der IMSI-Catcher insoweit also erfolgreich sein, müsste die G 10-Kommission bei Anschlussmaßnahmen beteiligt werden. Sollte der IMSI-Catcher nicht zu einer Nummernidentifikation führen, wäre nur der

ursprüngliche, geringe Eingriff gegeben und eine Beteiligung der G 10-Kommission erschiene im Gesamtsystem nicht schlüssig. Der Gesetzgeber hat insoweit keine Differenzierung vorgenommen.[243]

Zudem ist festzustellen, dass bei einer TK-Bestandsdatenabfrage nach § 8d BVerfSchG ebenso die Telefonnummer des Betroffenen (nebst weiteren Vertragsdaten) abgefragt werden kann, ohne dass hierfür ein G 10-Verfahren erforderlich wäre. Wenn auch die Einsatzumstände nicht selten andere sind, so wird im Ergebnis bei beiden Maßnahmen die Telefonnummer ohne Wissen des Betroffenen abgefragt; allerdings ist die Drittbetroffenheit beim IMSI-Catcher höher, wenn auch insgesamt geringfügig[244].

Ferner stellt sich in der Anwendungspraxis nicht selten das Problem eines häufigen Wechsels der SIM-Karte oder des Mobiltelefons, weshalb die zeitlich aufwendigen IMSI-Catcher-Maßnahmen ins Leere laufen. Eine praktikable und zugleich systemgerechte Lösung wäre die Möglichkeit formerleichterter Anschlussmaßnahmen. Somit könnten durch eine Genehmigung der G 10-Kommission einerseits mehrere Identifikationsmaßnahmen gegen denselben Betroffenen in einem bestimmten Zeitraum durchgeführt werden, indem etwa mehrere Nummern lokalisiert werden. Zum anderen sollte die Genehmigung Anschlussmaßnahmen nach dem G 10 für alle mittels IMSI-Catcher ermittelten Nummern ermöglichen Ein ähnliches Problem zeigt sich in Fällen, in denen bereits ein G 10-Verfahren gegen den Betroffenen läuft und nur weitere Nummern identifiziert werden müssen, weil ein anderes als das überwachte Telefon genutzt wird.[245] Auch hier wäre es naheliegend, die Genehmigung der G 10-Kommission um notwendige Anschluss-Kennungen gegen denselben Betroffenen zu erweitern, einschließlich der Erlaubnis, auch gegen die nunmehr ermittelten Nummern G 10-Maßnahmen zu ergreifen. Schließlich wäre es jedenfalls bei Identifikation lediglich der Telefonnummer entsprechend der TK-Bestandsdatenabfrage nach § 8d BVerfSchG konsistent, auf eine Mitteilungspflicht zu verzichten.[246]

5.3.7. § 8a Abs. 2 S. 1 Nr. 3 a. F. BVerfSchG (Postdienstleister)

Die nachrichtendienstliche Praxis hat Anwendungsbereiche für § 8a Abs. 2 S.1 Nr. 3 a. F. BVerfSchG aufgezeigt. So wird etwa im Bereich Rechtsextremismus von Labels und Vertrieben berichtet, die über Postfächer und Packstationen operierten, aber auch von rechtsextremen Netzwerken in Haftanstalten, die über Briefe kommunizieren würden. Auch im Bereich Islamismus und Linksextremismus würden Informationen über Briefe und Postfächer ausgetauscht. Die Abschaffung allein wegen fehlender Nutzung im damaligen Erhebungszeitraum vermag nicht zu überzeugen, da die entscheidende Frage die ist, ob künftige Anwendungsfälle möglich sind. Selbstverständlich mag hier die Vergangenheit Indiz sein, doch ist sie auch nicht mehr. Ausweislich der Darstellung mehrerer Fachbereiche ist ein Bedarf gegeben. Die Abfrage bei Postdienstleistern würde sich deshalb in ein konsistentes System der Erforschung und Bekämpfung medienübergreifend agierender Zielpersonen einfügen.

---

[243] Der Gesetzgeber ging ursprünglich von einem Eingriff in Art. 10 GG aus und sah folgerichtig entsprechende Anforderungen vor, BT-Drs. 14/7386, S. 40. Im Zuge der Gesetzesevaluation ging er 2006 von einer „besonderen Grundrechtsbedeutung“ des IMSI-Catcher aus, weshalb er die ursprünglichen Kautelen beibehielt, ohne allerdings die grundrechtliche Bedeutung auszuführen, BT-Drs. 16/2921, S. 16. Das Ergebnis steht selbstverständlich im Ermessen des Gesetzgebers, doch vermag die Begründung jedenfalls in Bezug auf die Nummernidentifikation nicht zu überzeugen. Denn hier ist der Eingriff für sich äußerst gering und es besteht praktisch kein Missbrauchspotenzial, da die Anschlussmaßnahmen das G 10-Verfahrren vorsehen.

[244] BVerfG, Beschluss vom 22.08.2006, Az. 2 BvR 1345/03, juris, Rn 77.

[245] So auch Wolff, S. 100.

[246] Dazu, dass eine solche verfassungsrechtlich nicht geboten ist, vgl. BVerfG, NJW 2007, 351 (356).

Zudem ist zu beachten, dass die geringe Nutzung einer Eingriffsbefugnis die Intensität ihrer Freiheitsbeschränkung selbst reguliert: Je weniger die Norm aktiviert wird, desto geringer ist die grundrechtliche Belastung. Sollte tatsächlich niemand Postdienstleistungen nutzen, bestünde für niemanden das Risiko, nachrichtendienstlich überwacht zu werden. Soweit aber Postdienstleistungen von Zielpersonen genutzt werden, erhält die Befugnisnorm auch ihre Legitimation. Schließlich würde eine zu leichthändige Abschaffung nicht angewendeter Befugnisse einen Anreiz bei den Nachrichtendiensten für deren „Aktivierung“ schaffen, um die Befugnis auch künftig nutzen zu können. Umgekehrt kann eine geringe Nutzung auch als Ausdruck schonender Befugnisausübung interpretiert werden.

6. Fallstudienanalyse

In Abstimmung mit dem BMI und dem BfV erfolgte am 1. Juni 2017 eine Analyse ausgewählter TBG-Maßnahmen sowie einer IMSI-Catcher-Maßnahme, um zu prüfen, ob eine Fallstudie in Form einer Aktenanalyse das geeignete Mittel ist, um einen konkreten Einblick in das nachrichtendienstliche Vorgehen bei der Anordnung und vor allem bei der Weiterverwendung der gewonnen Informationen zu erlangen. Dies sollte gerade mit Blick auf Folgemaßnahmen (auch im Bereich des Law Enforcement) und additive Grundrechtseingriffe erfolgen.
Auf Grundlage des Fallstudienkonzepts vom 15. Mai 2017 wurde anhand von insgesamt fünf Anträgen gemäß § 8a BVerfSchG bzw. § 9 Abs. 4. BVerfSchG eine explorative Analyse im BfV in Köln durchgeführt. Bei den Anträgen handelte es sich um

- zwei besondere Auskunftsverlangen gemäß § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG (Telekommunikationsverkehrsdaten-Abfrage),
- einen Antrag gemäß § 9 Abs. 4 BVerfSchG (IMSI-Catcher-Einsatz),
- ein besonderes Auskunftsverlangen gemäß § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG bzw. § 8a Abs. 2a BVerfSchG (Kombi-Antrag Kontostamm- bzw. Finanztransferdaten-abfrage),
- ein besonderes Auskunftsverlangen gemäß § 8a Abs. 2 S. 1 Nr. 1 BVerfSchG (Flugdatenabfrage).

Die Anträge stammten aus unterschiedlichen Fachabteilungen. Die Auswahl erfolgte durch das BfV nach Maßgabe des Evaluationskonzeptes (abgeschlossene/beendete Maßnahmen aus den Jahren 2014/2015) unter Berücksichtigung der VS-Einstufung und der Sensibilität der Informationen. Es handelte sich um Fälle aus den Phänomenbereichen Rechtsextremismus, Islamismus/islamistischer Terrorismus sowie Ausländerextremismus und Linksextremismus/-terrorismus. Da die dem InGFA vorgelegten Schriftstücke als Verschlusssache GEHEIM eingestuft waren, durften keine Aufzeichnungen erstellt werden, die Informationen zum konkreten Sachverhalt enthalten. Die Analyse der ausgewählten Fälle beschränkte sich somit darauf, einen Überblick über die Struktur solcher Anträge zu erhalten.
Anhand der explorativen Analyse wurde deutlich, dass die untersuchten Anträge durch einen hohen Standardisierungsgrad gekennzeichnet sind. Folgende Struktur war bei allen Anträgen zu finden:

1. Kurzübersicht/Betroffene der Maßnahme
2. Anlass
3. Tatsächliche Anhaltspunkte
4. Aktuelle Erkenntnisse (soweit vorhanden)
5. Begründung der Erforderlichkeit
6. Beweisliste (nicht Bestandteil der zur Verfügung gestellten Unterlagen)
7. Ansprechpartner für Rückfragen (in der Regel Referatsleiter und Sachbearbeiter)

Bei allen fünf Maßnahmen zeigte sich, dass eine umfangreiche Darlegung des Sachverhalts und der Erforderlichkeit erfolgte, wobei eine tiefergehende Prüfung dieser Darstellungen durch

das InGFA nicht möglich war, da die Beweismittel nicht Bestandteil der zur Verfügung gestellten Unterlagen waren.[247]

Anhand der Sachverhaltsdarstellungen ließ sich erkennen, dass im Vorfeld einer solchen Maßnahme bereits verschiedene nachrichtendienstliche Mittel der Informationserhebung (Observationen, SIS-Ausschreibungen, Hinweise ausländischer Nachrichtendienste etc.) genutzt wurden. Hingegen konnten die zur Verfügung gestellten Akten keine Erkenntnisse zur Weiterverwendung der durch die jeweilige Maßnahme gewonnenen Informationen liefern. Dies hat folgende Ursachen: Den Bearbeitern wurden lediglich die Anträge zur Verfügung gestellt, aus denen sich der Erfolg und die Folgen der Maßnahme nicht erkennen ließen. Vollakten waren aus Geheimschutzgründen nicht einsehbar. Zudem kann eine Kumulation von Maßnahmen kaum erkannt werden, da zum einen viele Betroffene Aliasse führen und deshalb mehrere Akten angelegt wurden. Zum anderen müsste eine volle Abbildung kumulierter Eingriffe alle Sicherheitsbehörden erfassen, was praktisch ausgeschlossen ist. Damit sind kumulative Eingriffe durch nicht-koordinierte Maßnahmen der Sicherheitsbehörden für niemanden ersichtlich. Schließlich werden die Maßnahmen des Law Enforcement von den Nachrichtendiensten nicht erfasst, sodass auch insoweit eine Erhebung ausgeschlossen ist. Lediglich bei den durch den Einsatz des IMSI-Catchers gewonnenen Informationen war eine Folgemaßnahme ersichtlich. Dies liegt aber in der Natur des IMSI-Catchers begründet und lässt keinen Rückschluss auf mögliche Probleme kumulativer Grundrechtseingriffe oder auf den Umgang mit Daten über die Zeit zu.

Insgesamt lässt sich jedoch eine hohe Normgeleitetheit und daran orientierte Standardisierung und Auseinandersetzung bei den untersuchten Fällen erkennen.

[247] Eine Vorlage der Beweismittel war entsprechend dem Evaluationsauftrag auch nicht notwendig, da die Rechtmäßigkeit der Anordnungen und die Entscheidungen der G 10-Kommission nicht Gegenstand der Evaluierung waren.

7. Zusammenfassung der Ergebnisse

(1) § 3 Abs. 1 Nr. 4 BVerfSchG, § 5 Abs. 2 BVerfSchG, § 1 Abs. 1 S. 2 MADG

Eine empirische Analyse von § 3 Abs. 1 Nr. 4 BVerfSchG, die alle Tätigkeitsbereiche des BfV umfasst, war im Rahmen des Evaluationsvorhabens aufgrund des immensen Aufwands, der mit der statistischen Erfassung *aller* Anwendungsfälle für das BfV verbunden gewesen wäre, nicht möglich. Jedoch lassen sich in Kombination mit den ebenfalls evaluierungspflichtigen Regelungen § 8a BVerfSchG und § 9 Abs. 4 BVerfSchG Hinweise auf die praktische Anwendung der Norm gewinnen. Hiernach hat die Einfügung von § 3 Abs. 1 Nr. 4 BVerfSchG nicht dazu geführt, dass im umfangreichen Maße zusätzliche Datenerhebungsmaßnahmen gemäß § 8a Abs. 2 und 2a BVerfSchG sowie § 9 Abs. 4 BVerfSchG durchgeführt wurden. Zwar wurde eine nicht unerhebliche Anzahl von Maßnahmen zusätzlich auf Nummer 4 gestützt. Als alleinige Grundlage für das Tätigwerden des BfV diente § 3 Abs. 1 Nr. 4 BVerfSchG allerdings in keinem Fall. Für § 1 Abs.1 S. 2 MADG stellt sich die Situation ähnlich dar. Ein kleiner Teil der durchgeführten nachrichtendienstlichen Operationen (v. a. im Bereich Islamismus und Ausländerextremismus) stützte sich auf diesen Teil der Aufgabennorm. Beim Großteil seiner Aktivitäten griff das BAMAD hingegen auf § 1 Abs. 1 S. 1 MADG zurück. In dieser ergänzenden Funktion werden die Neuregelungen sowohl von BfV als auch von BAMAD als sinnvoll angesehen. Die verfassungsrechtliche Bewertung der Anwendungspraxis kommt zu dem Schluss, dass beide Normen zur Erreichung des mit ihnen verfolgten Ziels sowohl geeignet als auch erforderlich sind. Die lediglich supplementär und sehr zurückhaltend erfolgende Nutzung der eingefügten Aufgabennormen durch BfV und BAMAD, deutet daraufhin, dass die nachrichtendienstliche Praxis sich innerhalb der durch die Anforderungen der Angemessenheit gezogenen Grenzen bewegt.

(2) § 8a-c BVerfSchG, § 3 BNDG, § 4a MADG

§ 8a Abs. 1 BVerfSchG, § 3 BNDG und § 4a MADG

Das Instrument der Bestandsdatenabfrage bei Teledienstanbietern wurde vom BfV gegenüber dem letzten Berichtszeitraum deutlich häufiger genutzt (251 statt zwölf Fälle), während es bei BND und BAMAD im Erhebungszeitraum weiterhin nicht zur Anwendung kam. Die Anwendungspraxis zeigte nur geringe Probleme – etwa bei der Verarbeitung unterschiedlicher Dateiformate – in der Zusammenarbeit mit den verpflichteten Unternehmen und die Bestandsdatenabfrage wird als wichtige Maßnahme angesehen, etwa um Facebook-Konten, auf denen IS-Flaggen zu sehen waren, zu überprüfen. Auch BAMAD und BND sehen hier wichtige Anwendungsbereiche.
Der erhebliche Anstieg der Bestandsdatenabfragen lässt keinen Schluss auf eine gleichsam flächenmäßige, den Rahmen der Angemessenheit verlassende Nutzung zu, da sich insoweit das Nutzungsverhalten der Betroffenen und die allgemeine Sicherheitslage entscheidend verändert, aber auch die Abläufe des Anordnungsverfahrens im BfV sich eingespielt haben.

§ 8a Abs. 2 und 2a BVerfSchG, § 3 BNDG und § 4a MADG

Das Nutzungsverhalten der Nachrichtendienste hinsichtlich der besonderen Auskunftsverlangen fällt sehr unterschiedlich aus. Bislang wurden die Befugnisse in erster Linie vom BfV genutzt, während BND und BAMAD nur in Ausnahmefällen darauf zurückgegriffen haben. Dies liegt vor allem daran, dass beim BND aufgrund des Auslandsbezugs der Tätigkeit sowie beim BAMAD aufgrund der Beschränkung der Zuständigkeit auf den Geschäftsbereich des BMVg die Instrumente eher selten zum Einsatz kommen können.

Im überwiegenden Teil der Fälle ging es um die Abfrage von Verkehrsdaten bei Telekommunikationsdiensteanbietern (§ 8a Abs. 2 S. 1 Nr. 4 BVerfSchG) sowie um Abfragen bei Kreditinstituten, Finanzunternehmen, Finanzdienstleistungsunternehmen und beim BZSt – sog. Kombi-Anträge (§ 8a Abs. 2 S. 1 Nr. 2 und Abs. 2a BVerfSchG). Nicht in Anspruch genommen wurde hingegen die Möglichkeit, Verkehrsdaten bei Teledienstanbietern abzufragen (§ 8a Abs. 2 S. 1 Nr. 5 BVerfSchG). Lediglich einmal erfolgte eine Flugdatenabfrage (durch das BAMAD). Die Maßnahmen wurden hauptsächlich auf § 3 Abs. 1 Nr. 1, Nr. 3 und Nr. 4 BVerfSchG gestützt, wobei in der Mehrzahl der Fälle mehrere Gründe angegeben wurden.
Wichtigster Phänomenbereich war mit Abstand der Islamismus, gefolgt von Proliferation und Spionage sowie Rechts-/Linksextremismus. Die Anordnungen richteten sich gegen 110 Personen (81 Haupt- und 29 Nebenbetroffene). Hinsichtlich der im Rahmen der besonderen Auskunftsverlangen gewonnenen Daten wurde deutlich, dass mit Blick auf den Datenumfang vor allem TK-Verkehrsdaten und Finanzermittlungsmaßnahmen im Erhebungszeitraum eine große Rolle spielten, da hierbei insgesamt die meisten Informationen erhoben wurden (z. B. Anschlussnummern, Standortdaten, Verbindungsdaten, Kontonummern, Inhaber, Kontostände. etc.). Festzuhalten ist darüber hinaus, dass es im Erhebungszeitraum kaum zu Problemen bei der Erteilung der Auskünfte gekommen ist. Dies spiegelt sich auch in der Bewertung der Reaktionszeit der Unternehmen durch die Nachrichtendienste wider, die im Großteil der Fälle als schnell bzw. sehr schnell eingeschätzt wurde.
Nach Einschätzung der Nachrichtendienste sind die besonderen Auskunftsverlangen ein wichtiges und wertvolles Instrument für die nachrichtendienstliche Arbeit. Die Ausdehnung der Befugnisse gemäß § 8a Abs. 2 S. 1 Nr. 1 BVerfSchG auf Computerreservierungssysteme und Globale Distributionssysteme wird von allen Nachrichtendiensten positiv bewertet. Ebenfalls positiv bewertet wurde die Möglichkeit zur Kontostammdatenabfrage beim BZSt bzw. zur Stellung eines Kombi-Antrags. Dadurch konnte der Arbeitsablauf im Zusammenhang mit der Kontenüberprüfung deutlich vereinfacht und beschleunigt werden. Zudem ergeben sich bessere Analysemöglichkeiten, sodass das Instrument der Finanzermittlungen deutlich an Aussagekraft gewonnen hat. Bei der Abfrage von Verkehrsdaten bei Telekommunikationsunternehmen handelt es sich aus Sicht der Nachrichtendienste ebenfalls um ein wichtiges Instrument zur Gewinnung von werthaltigen Informationen zum Kommunikationsverhalten einer Zielperson. Darüber hinaus stellt das Instrument eine weniger eingriffsintensive Maßnahme als die Inhaltsüberwachung dar. Sowohl die Maßnahmen gemäß § 8a Abs. 2 S. 1 Nr. 2 in Verbindung mit § 8a Abs. 2a BVerfSchG als auch die Maßnahme nach § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG werden häufig dazu genutzt, um G 10-Maßnahmen einzuleiten bzw. besser und gezielter vorzubereiten. Maßnahmen nach § 8a Abs. 2 S. 1 Nr. 2 in Verbindung mit § 8a Abs. 2a BVerfSchG dienen hingegen dazu, die Ermittlungen zielgerichtet auf das Finanzverhalten der Betroffenen abzustellen.
Kritik wurde von den Nachrichtendiensten vor allem an der Ausgestaltung des Mitteilungsregimes geäußert. Zum einen sei es fraglich, ob bei wenig grundrechtsintensiven Maßnahmen nach § 8a Abs. 1 und Abs. 2a BVerfSchG überhaupt eine Mitteilungspflicht bestehen müsse. Zum anderen müsse aber, ebenso wie bei einzelnen Auskunftsverlangen nach § 8a Abs. 2 BVerfSchG, eine endgültige Nichtmitteilung möglich sein. Ferner seien die tatbestandlichen Anforderungen an Bestandsdatenabfragen bei Telediensteanbietern und Kontostammdatenabfragen unpraktikabel hoch. Ferner regen die Nachrichtendienste eine Wiedereinführung der Abfrage bei Postdienstleistern (§ 8a Abs. 2 S. 1 Nr. 3 a. F.) an, da es hierfür Anwendungsfälle gebe.
Anhaltspunkte, die die Geeignetheit oder Erforderlichkeit der von den Nachrichtendiensten auf der Grundlage dieser Vorschriften ergriffenen Maßnahmen zur Abwehr von Gefahren für die

in § 3 Abs. 1 BVerfSchG genannten Schutzgüter in Frage stellen, ergeben sich aus der empirischen Erhebung nicht. Auch wenn die Zahl der Bestandsdatenabfragen bei Teledienste-anbietern im Vergleich zum letzten Berichtszeitraum erheblich gestiegen ist, bewegt sich die Zahl mit etwa 20 Anordnungen pro Monat deutlich unterhalb eines flächendeckenden Niveaus. In Anbetracht dessen, dass § 8a Abs. 2 und Abs. 2a BVerfSchG zu einer Reihe von Auskunfts-verlangen ermächtigen, ist die Zahl der durch alle Nachrichtendienste des Bundes insgesamt nach diesen Vorschriften durchgeführten Auskunftsverlangen nicht sehr hoch, was auf eine zurückhaltende Nutzung dieser Maßnahmen schließen lässt.

§ 8b BVerfSchG, § 3 BNDG und § 4a MADG

Da es im Erhebungszeitraum wegen der zur Gewährleistung effektiven Rechtsschutzes bestehenden Notwendigkeit, die seitens der Nachrichtendienste durch Anordnungen nach § 8 Abs. 2 und 2a BVerfSchG erhobenen Informationen zur Auswertung bzw. zur Dokumentation für eventuelle gerichtliche Verfahren noch vorzuhalten, zu keiner Löschung von Daten gekommen ist, ist eine verfassungsrechtliche Bewertung der Praxis der Anwendung von § 8b Abs. 2 S. 7 BVerfSchG nicht möglich.
Die Mitteilung an Betroffene nach § 8b Abs. 7 BVerfSchG ist seitens der Nachrichtendienste in beträchtlichem Umfang erfolgt. Das Unterbleiben einer Mitteilung bedarf in jedem Einzelfall einer besonderen Begründung des Bestehens einer Gefährdung des Zwecks der Maßnahme oder des Eintritts übergreifender Nachteile für das Wohl des Bundes oder eines Landes. Verfassungswidrige Verkürzungen der Rechte der Betroffenen können daher nicht festgestellt werden.

(3) § 9 Abs. 4 BVerfSchG, § 5 BNDG, § 5 MADG

Im Erhebungszeitraum wurde der IMSI-Catcher 18-mal vom BfV angeordnet.[248] Hauptgründe für den Einsatz waren dabei zum einen Hinweise auf Bestrebungen, die gegen die freiheitlich demokratische Grundordnung gerichtet waren, und zum anderen Hinweise auf Bestrebungen, die durch die Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährdeten bzw. Bestrebungen, die gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 GG), insbesondere gegen das friedliche Zusammenleben der Völker (Art. 26 Abs. 1 GG) gerichtet waren. Der IMSI-Catcher wurde hauptsächlich im Bereich des Islamismus, gefolgt von Proliferation und Spionage und Rechts-/Linksextremismus eingesetzt. Die Anordnung der Maßnahme richtete sich im Erhebungszeitraum gegen 23 Hauptbetroffene und einen Nebenbetroffenen. Der IMSI-Catcher wurde dabei hauptsächlich zur Erfassung der Geräte- und Kartennummern genutzt. Darüber hinaus wurden in zwei Fällen zusätzlich die Standortdaten erfasst. In 17 Fällen des BfV betrug der in der Anordnung festgelegte Zeitraum für die Nutzung des IMSI-Catchers drei Monate, wobei er in der Regel nur einmal eingesetzt wurde und die Dauer des Einsatzes zwischen einem und sieben Tagen variierte. Insgesamt wird der Nutzen der mit Hilfe der Maß-nahme gewonnenen Daten für die nachrichtendienstliche Arbeit als hoch bzw. sehr hoch ein-gestuft. Somit ist der IMSI-Catcher aus Sicht der Nachrichtendienste ein sinnvolles und nützliches Instrument der Informationsgewinnung, mit dem gezielt Nummern erfasst werden können, um damit zusätzliche G 10-Maßnahmen vorzubereiten. Dies gelte insbesondere für Personen, die damit rechnen, überwacht zu werden und deshalb neue SIM-Karten nutzen.

[248] Allerdings wurden nur 16 Anordnungen umgesetzt.

Die Maßnahme dient dem Schutz hochrangiger verfassungsrechtlicher Güter, wie sie in § 3 Abs. 1 BVerfSchG normiert sind. Die aus der empirischen Erhebung ermittelte Anwendungspraxis enthält keine Anhaltspunkte, dass der Einsatz des IMSI-Catchers ungeeignet zur Erreichung des Schutzes dieser Güter war. Hinweise darauf, dass die sich aus der gebotenen Verhältnismäßigkeit im engeren Sinne ergebenden Anforderungen durch Maßnahmen nach § 9 Abs. 4 BVerfSchG verfehlt worden sind, sind nicht erkennbar. Die Anordnungen sind offenbar auf das zur Zweckerreichung unabdingbare Maß beschränkt worden, sowohl hinsichtlich der regelmäßigen Erstreckung auf nur eine Person sowie hinsichtlich der typischen Beschränkung der Erfassung auf die Geräte- und Kartennummern unter Nichterfassung von Standortdaten als auch mit Blick auf die zeitliche Beschränkung des IMSI-Catcher-Einsatzes innerhalb der Befristung der Anordnung.

(4) § 12 Abs. 3 BVerfSchG, § 20 Abs. 1 BNDG, § 6 Abs. 2 MADG

Im Erhebungszeitraum gab es keinen Fall, in dem ein Antrag auf Nichtlöschung personenbezogener Daten gestellt wurde. Das BfV befürwortete grundsätzlich eine Verlängerung der Höchstspeicherdauer auf 15 Jahre für bestimmte Personengruppen (z. B. Personen im Untergrund/Ausland). Für eine Verlängerung sprach sich auch das BAMAD aus, um den geänderten Erwerbsbiographien von Angehörigen des Geschäftsbereichs Rechnung zu tragen. Der BND wendete die Höchstfrist aus teleologischen und systematischen Gründen nicht an und prüfte stattdessen regelmäßig (allein) die Erforderlichkeit der Datenhaltung. Die empirisch erhobene Anwendungspraxis wirft mit Blick auf das Grundrecht auf informationelle Selbstbestimmung keinen verfassungsrechtlichen Erörterungsbedarf auf.

(5) § 17 Abs. 3 BVerfSchG

Im Erhebungszeitraum wurden hauptsächlich Personen im SIS II ausgeschrieben. Übermittelt wurden in erster Linie Informationen zu Ort, Zeit oder Anlass der Kontrolle, zum Auffinden der Person sowie zum Reiseweg und -ziel. In mehr als 50 Prozent der Fälle stammten die übermittelten Informationen aus Deutschland. Im überwiegenden Teil der Fälle dienten die SIS II-Ausschreibungen dazu, Informationen zu gewinnen, die zur Abwehr anderer erheblicher Gefahren für die innere oder äußere Sicherheit erforderlich waren. Die Möglichkeit, Personen bzw. Sachen im SIS II auszuschreiben, wurde insgesamt 818 Mal und dabei hauptsächlich vom BND und BfV und deutlich weniger intensiv vom BAMAD genutzt. Hinsichtlich der Ausschreibungspraxis ist festzustellen, dass bei fast allen Ausschreibungen im Erhebungszeitraum die maximale Befristungsdauer von sechs Monaten ausgeschöpft wurde. In acht von zehn Fällen kam es zu einer wiederholten Anordnung der Ausschreibung.
In ca. 35 Prozent der Fälle über alle Nachrichtendienste hinweg wurde die ausgeschriebene Person bzw. Sache angetroffen. Die Bewertung der im Rahmen der Ausschreibung gewonnenen Informationen für die Arbeit des BfV fiel differenziert aus. In den Fällen, in denen ein Treffer erfolgte (50 Prozent), wurde der Nutzen der übermittelten Informationen überwiegend als hoch bzw. sehr hoch eingestuft. In den Fällen, in denen die ausgeschriebene Person bzw. Sache nicht angetroffen wurde, wurde der Nutzen dagegen überwiegend als gering bzw. sehr gering eingestuft. Beim BND war die Trefferquote mit 26 Prozent deutlich geringer als beim BfV. Zudem fiel die Bewertung insgesamt eher verhalten aus, da in allen Fällen der Nutzen der im Rahmen der Ausschreibung gewonnenen Informationen für die nachrichtendienstliche Arbeit mit „teils/teils“ eingestuft wurde.
Insgesamt ist festzuhalten, dass die SIS II-Ausschreibungen gemäß § 17 Abs. 3 BVerfSchG aus Sicht der Nachrichtendienste ein wichtiges Instrument für die Erstellung von Reiseprofilen

darstellen. Kam es zu einem Treffer, war der Nutzen der im Rahmen der Ausschreibung gewonnenen Informationen für die Arbeit von BfV und BAMAD im Großteil der Fälle hoch bzw. sehr hoch. Aber auch die Fälle, die – oft trotz wiederholter Ausschreibung – zu keinen Trefferm eldungen führen, können manchmal wertvolle Informationen liefern.
Dementsprechend können die durchgeführten Ausschreibungen nicht als ungeeignet zur Erreichung der mit ihnen verfolgten Ziele angesehen werden. Ein milderes Mittel, diese Ziele gleich wirksam zu erreichen, ist insbesondere für die Gewinnung von Informationen aus dem europäischen Ausland nicht erkennbar. Die empirische Erhebung lässt eine unverhältnismäßige Handhabung nicht erkennen. Allein die faktische Belastung der Betroffenen durch die Ausschreibung (indirekte Markierung für ausländische Nachrichtendienste) wirft einen möglichen Anpassungsbedarf auf.

(6) § 18 Abs. 1a BVerfSchG

Im Erhebungszeitraum kam § 18 Abs. 1a BVerfSchG deutlich häufiger als im letzten Berichtszeitraum zur Anwendung (2016/17: 4.787; 2013/14: 200 Fälle). Der weit überwiegende Teil erfolgte mit ca. 80 Prozent im Bereich Islamismus, gefolgt von Ausländer-/Linksextremismus und Spionageabwehr/Proliferation. Die übermittelten Informationen wurden, je nach Phänomenbereich, in äußerst unterschiedlichem Umfang gespeichert: von 3,5 Prozent im Bereich Spionageabwehr/Proliferation über 41,1 Prozent bei Ausländer- und Linksextremismus bis zu 88,3 Prozent bei Islamismus. Die hohen Übermittlungszahlen und Speicherquoten im Bereich Islamismus wurden v. a. mit der geänderten Sicherheitslage und einer anderen Aufmerksamkeit beim BAMF begründet. Die Ersthinweise des BAMF werden vom BfV als wichtig eingeschätzt, um relevante Informationen zu möglichen Gefährdern zu erhalten, die etwa die Ziele des IS in Deutschland weiterverfolgen wollen.
Aus verfassungsrechtlicher Sicht kann die Übermittlung der teils sensiblen Informationen ohne Weiteres durch die hohen Schutzgüter gerechtfertigt sein. Allein die derzeit offenbar nur unzureichende Filterung durch das BAMF bedarf einer Anpassung.
Nur im Bereich Islamismus wurden Informationen im Einzelfall an ausländische Partnerdienste übermittelt.
Auf Bundesländerebene erfolgten Spontanübermittlungen gemäß § 18 Abs. 1a BVerfSchG eher im Einzelfall, wobei im Vergleich mit den Nachrichtendiensten des Bundes das unterschiedliche Aufgabenprofil zu beachten ist. Hinsichtlich des Speicherverhaltens ergibt sich auf Bundesländerebene ein deutlich anderes Bild als auf Bundesebene. In nur etwas mehr als 14 Prozent der Fälle kam es zu einer Speicherung von Informationen bei den zuständigen Landesverfassungsschutzbehörden. Die Bewertung des konkreten Nutzens für die Arbeit der Landesverfassungsschutzbehörden fiel sehr durchwachsen aus.
In Anbetracht der Tatsache, dass Übermittlungen durch die Ausländerbehörden der Länder an die Landesverfassungsschutzbehörden deutlich zurückhaltender als Übermittlungen des BAMF an das BfV erfolgten, besteht ebenfalls kein Anlass zu verfassungsrechtlichen Zweifeln an der empirisch erhobenen Übermittlungspraxis.

(7) § 19 Abs. 4 und 5 BVerfSchG, § 11 Abs. 1 S. 1 MADG

Hinsichtlich der Übermittlung personenbezogener Daten zur Gewährleistung der Sicherheit von lebens- und verteidigungswichtigen Einrichtungen nach § 1 Abs. 4 SÜG verwiesen BfV und BAMAD darauf, dass es sich um absolute Einzelfälle handele. Im Erhebungszeitraum sei es zu keiner Übermittlung gekommen.
Die Anwendung von § 19 Abs. 5 BVerfSchG gehört zur täglichen Arbeit des BfV und des BAMAD, da es bei der Sammlung von Informationen notwendig sein kann, einer anderen

Stelle (z.B. Hotel/Mietwagenfirma) den Namen der Zielperson zu nennen, um weiterführende Informationen zu erhalten.
Die empirische Auswertung der nachrichtendienstlichen Praxis hat keine Hinweise darauf ergeben, dass die in den evaluierten Regelungen statuierten Ausnahmen zur Sicherung der Wirksamkeit nachrichtendienstlicher Maßnahmen in die verfassungsrechtlichen Grenzen verletzender Weise angewandt worden sind.

(8) § 10 Abs. 1 und 3 MADG

Im Evaluationszeitraum sind keine Fälle gemäß § 10 Abs. 1 und Abs. 3 MADG aufgetreten. Nach Angabe des BfV und des BAMAD beziehen sich die Regelungen auf einen sehr kleinen Anwendungsbereich. Es handele sich lediglich um Folgeänderungen aufgrund des neueingefügten § 1 Abs. 1 S. 2 MADG. Mangels dokumentierter Fälle ist eine verfassungsrechtliche Bewertung der Anwendungspraxis nicht möglich.

(9) § 11 Abs. 1 S. 3 MADG

Im Erhebungszeitraum erfolgte keine Weitergabe der personenbezogenen Daten gemäß § 11 Abs. 1 S. 3 i. V. m. § 18 Abs. 1a BVerfSchG an ausländische öffentliche Stellen bzw. an über- und zwischenstaatliche Stellen.

(10) § 24 Abs. 1 und 2 BNDG (§ 9 Abs. 1 und 2 BNDG a. F.)

Im Evaluationszeitraum hatte die Änderung des § 9 Abs. 1 und 2 BNDG a. F. für die Tätigkeit des BND keine Bedeutung.

(11) § 1 Abs. 4 und 5 SÜG

Mit der gesetzlichen Fixierung der Zielsetzung im Änderungsgesetz 2011, die mit dem vorbeugenden personellen Sabotageschutz verfolgt wird, kam es auch zur Einführung einer erweiterten SÜ. Zwischen 2015 und 2017 wurden im nichtöffentlichen Bereich 14.736 SÜ vps eingeleitet und 14.272 abgeschlossen, im öffentlichen Bereich 10.317 eingeleitet und 10.768 abgeschlossen und im militärischen Sicherheitsbereich 45.673 eingeleitet und 50.505 abgeschlossen. Die Zusammenfassung folgt den drei Bereichen.
Im *nichtöffentlichen Bereich* hat sich sowohl das Verfahren trotz des hohen Aufwandes und einzelnen Verbesserungsbedarfen als auch die Harmonisierung des vorbeugenden personellen Sabotageschutzes mit den Überprüfungssystemen aus Luft- und Atomsicherheit insgesamt bewährt. Das Überprüfungsverfahren wurde rechtlich wie organisatorisch leicht angepasst, die Zusammenarbeit von Sabotageschutzbeauftragten, BMWi als zuständiger Stelle und BfV als mitwirkender Behörde funktioniert insgesamt gut. Allerdings gab das BMWi zu bedenken, es könne die Frage gestellt werden, ob der hohe Aufwand in einem angemessenen Verhältnis zum Nutzen stehe. Besondere Probleme ergaben sich laut BMWi-Fachreferat zum einen dadurch, dass immer wieder eine abgeschlossene SÜ als Voraussetzung für die Teilnahme am Bieterwettbewerb gefordert würde, und zum anderen durch die hohe Fluktuation des Personals bei Fremdfirmen.
Im *öffentlichen Bereich* hat sich das Verfahren ebenfalls gut eingespielt. Aus Sicht des BMI-Fachreferats ergebe sich Optimierungsbedarf v. a. wegen der fehlenden Gleichwertigkeit der SÜ vpS mit der Ü2-Geheimschutz. Zum einen würden wichtige Informationen nicht abgefragt (keine Abfrage von Kontakten zu ausländischen Nachrichtendiensten in der Sicherheitserklärung und keine Einbeziehung des Partners der zu überprüfenden Person). Zum anderen werde die SÜ vpS in einigen Bundesländern nicht anerkannt, sodass es immer wieder zu Doppelüberprüfungen komme.

Im *militärischen Sicherheitsbereich* stellt sich die Akteurskonstellation etwas komplexer dar: Die SiBe leiten das Verfahren ein und betreuen es vor Ort. Das BAMAD ist mitwirkende Behörde. Sollte es zu sicherheitsrelevanten Erkenntnissen kommen, entscheidet hierüber der zuständige Geheimschutzbeauftragte, wobei die SiBe die Umsetzung der Entscheidung (etwa von Auflagen) vor Ort überwachen. Nach Ansicht des zuständigen BMVg-Fachreferates habe sich das SÜ-Regime bewährt, wobei die Auswirkungen der neu eingeführten Soldateneinstellungsüberprüfung abgewartet werden müssten. Hier sei allerdings mittelfristig mit einer Vereinfachung für den vpS zu rechnen, da auf die Ergebnisse der Einstellungsüberprüfung aufgebaut und Soldaten mit der erlangten Ü1 bis zum erfolgreichen Abschluss einer SÜ vpS ggf. auch nach § 15 SÜG vorläufig in entsprechenden militärischen Sicherheitsbereichen eingesetzt werden könnten.
Dank der Befragung der Sabotageschutz- bzw. Sicherheitsbeauftragten konnten zusätzliche Erkenntnisse (z. B. über die Anwendung der vpS-Regelungen in den drei Bereichen) gewonnenen werden. Die erweiterte Ausnahmeregelung wurde in allen Bereichen genutzt, jedoch in unterschiedlichem Umfang. Zudem zeigten auch bei der Relevanzbewertung z. T. deutliche Unterschiede zwischen den drei Bereichen. Der Aufwand des vpS wurde über alle Bereiche äußerst unterschiedlich eingeschätzt, wenn auch nur relativ wenige Stellen einen hohen oder sehr hohen Aufwand attestieren. Die Zusammenarbeit mit den mitwirkenden Behörden (BfV, BAMAD) wurde bereichsübergreifend als sehr positiv bewertet, wenn auch teilweise die langen Verfahrensdauern moniert wurden.
Aufgrund der hohen Schutzgüter des vpS stellen sich im Ergebnis keine verfassungsrechtlichen Bedenken. Angesichts des erheblichen Umfangs an Überprüfungen im nichtöffentlichen Bereich und den damit einhergehenden Belastungen für Unternehmen, Überprüfte, zuständige Stelle und mitwirkende Behörde kann die extrem geringe Zahl an Fällen mit festgestelltem Sicherheitsrisiko (ein Fall) durchaus die Frage nach dem angemessenen Nutzen aufwerfen. Zudem bedarf die Einstufung als lebens- und verteidigungswichtige Einrichtung angesichts der damit einhergehenden Folgen für Unternehmen sowie Mitarbeiterinnen und Mitarbeiter, aber auch wegen des behördlichen Aufwandes, einer fortwährenden Überprüfung.

8. Literaturverzeichnis

Bäumler, Helmut: Mitteilungen über Erkenntnisse des Verfassungsschutzes an Arbeitgeber, in: NVwZ 1999, S. 855-856.

Bender, Dominik: „Verpolizeilichung“ des Ausländerrechts?, in: KJ 2003, S. 130-145.

BMI – Bundesministerium des Innern: Bericht der Bundesregierung zum Ergebnis der Evaluierung nach Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007, 2011.

Bundesregierung: Bericht der Bundesregierung zu den Auswirkungen der nach Artikel 22 Abs. 2 des Terrorismusbekämpfungsgesetzes befristeten Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Artikel 10-Gesetzes, des Sicherheitsüberprüfungsgesetzes und des § 7 Abs. 2 des BKA-Gesetzes, 2005.

Droste, Bernadette: Handbuch des Verfassungsschutzrechts, Stuttgart u. a., 2007.

Gnüchtel, Ralf: Das Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen auf Grundlage der dritten Evaluation, in: NVwZ 1-2/2016, S. 13-16.

Harnisch, Stefanie/Pohlmann, Martin: Der Einsatz des IMSI-Catchers zur Terrorismusbekämpfung durch das Bundeskriminalamt, in: NVwZ 2009, S.1328-1332.

Hillgruber, Christian: Grundrechtlicher Schutzbereich, Grundrechtsausgestaltung und Grundrechtseingriff, in: Isensee, Josef/Kirchhof, Paul (Hrsg.): Handbuch des Staatsrechts der Bundesrepublik Deutschland. Band IX: Allgemeine Grundrechtslehren, 3. Auflage, Heidelberg, 2011, § 200.

Huber, Bertold: Das Bankgeheimnis der Nachrichtendienste. Zur Neuregelung der Auskunftsersuchen der Nachrichtendienste durch das Terrorismusbekämpfungsergänzungsgesetz vom 9. 1. 2007, in: NJW 2007, S. 881-883.

Lisken, Hans/Denninger, Erhard: Handbuch des Polizeirechts. Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 5. Auflage, München, 2012.

Lücke, Jörg: Der additive Grundrechtseingriff sowie das Verbot der übermäßigen Gesamtbelastung des Bürgers, in: DVBl 2001, S. 1469-1478.

Middel, Stefan: Innere Sicherheit und präventive Terrorismusbekämpfung, Dissertation, Baden-Baden, 2007.

Roggan, Fredrik/Kutscha, Martin: Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, Berlin, 2006.

Säcker, Franz Jürgen: Telekommunikationsgesetz, Kommentar, 3. Auflage, Frankfurt am Main, 2013.

Schenke, Wolf-Rüdiger/Graulich, Kurt/Ruthig, Josef: Sicherheitsrecht des Bundes, Kommentar, München, 2014.

Scheurle, Klaus-Dieter/Mayen, Thomas: Telekommunikationsgesetz, Kommentar, 2. Auflage, München, 2008.

Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 1. Auflage, Frankfurt am Main, 2010.

Tuffner, Martin: Das Schengener Informationssystem (SIS) – ein „Quantensprung“ der polizeilichen Fahndung in Europa, in: Bundeskriminalamt (Hrsg.): Festschrift für Horst Herold zum 75. Geburtstag, Wiesbaden, 1998, S. 239-257.

Von Mangoldt, Hermann/Klein, Friedrich/Starck, Christian: Kommentar zum Grundgesetz, Band 1: Präambel, Artikel 1 bis 19, Band 2: Artikel 20 bis 82, Band 3: Art. 83 bis 146, 6. Auflage, München, 2010.

Wolff, Heinrich Amadeus: Verfassungsrechtliche Bewertung des Terrorismusbekämpfungsergänzungsgesetzes (TBEG) und seiner Anwendung, Rechtsgutachten, 2011.

Wolff, Heinrich Amadeus/Mundil, Daniel: Die Verlängerung der speziellen Auskunftsbefugnisse der Nachrichtendienste, in: ZG 2012, S. 278-292.

9. Anhang

9.1. Konkrete Fallbeispiele für den Einsatz der Maßnahmen nach § 8a Abs. 2 und 2a BVerfSchG

9.1.1. Fallbeispiele zu § 8a Abs. 2 S. 1 Nr. 2 und Abs. 2a BVerfSchG

(1) Fallbeispiel 1 (BND)

Der BND stellte damals gemäß § 2a S. 1 BNDG [a. F.] i. V. m. § 8a Abs. 2 S. 1 Nr. 2 BVerfSchG ein besonderes Auskunftsersuchen zur Aufklärung eines internationalen Geldwäsche-Falles von erheblicher Bedeutung i. S. d. § 5 Abs. 1 S. 3 Nr. 6 G 10. Die damit eingeleitete Kontobewegungsabfrage zielte auf international agierende Netzwerke der Organisierten Kriminalität (OK). Die Maßnahme wurde im Rahmen einer Kooperation mit zwei weiteren EU-Nachrichtendiensten durchgeführt. Das Auskunftsersuchen richtete sich an ein deutsches Finanzinstitut (Sitz: Frankfurt/Main), das von besagten Netzwerken als Korrespondenzbank genutzt worden war. Im Ergebnis konnten dank der Anfrage jedenfalls die Transaktionen mit mutmaßlichem Geldwäschehintergrund als solche und die an den Transaktionen beteiligten Unternehmen eindeutig identifiziert werden. Darüber hinaus ermöglichte das Ergebnis dieses spezifischen Auskunftsersuchens Rückschlüsse auf weitere, zusätzlich involvierte Personen und/oder Gesellschaften. In der Folge wurden im EU-Ausland polizeilich-exekutive Maßnahmen durchgeführt. Solche Kontobewegungsabfragen stellen daher ein wertvolles Instrument dar, um Hintergrundinformationen zu illegalen Aktivitäten international agierender OK-Strukturen und Geldwäsche-Netzwerke, aber auch für transnational agierende Terrorstrukturen und deren Finanzströme zu gewinnen. Ihrer Natur nach dürften solche Abfragen v. a. Einzelinformationen i. S. v. „bits and pieces“ erbringen, die ein Lagebild aufgrund ihres dokumentarischen Charakters besonders belastbar ergänzen oder verifizieren bzw. falsifizieren. In dieser beschränkten, aber wichtigen Funktion liegt ihr ND-spezifischer Wert.

(2) Fallbeispiel 2 (BfV)

Die Maßnahme des BfV richtete sich gegen eine Person, die verdächtigt wurde, schwerwiegende Gefahren gegen die freiheitliche demokratische Grundordnung durch die Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen zu fördern. Im Rahmen von Demonstrationen rief ein rechtsextremistischer Personenzusammenschluss wiederholt offen zu einem gewaltsamen politischen Umsturz auf. Seine Mitglieder fielen immer wieder durch politisch motivierte Straftaten gegen Menschen mit Migrationshintergrund, vermeintliche linke Szeneangehörige und Polizeibeamte auf. Der Betroffene koordinierte in seiner Rolle als einer von mehreren Rädelsführern eines rechtsextremistischen Personenzusammenschlusses diverse Finanztransaktionen, welche den organisatorischen Zusammenhalt der Gruppierung nachdrücklich förderten (Beginn: März 2015).
Mit der Maßnahme, die im Juni 2015 endete, war es möglich, die Schlüsselrolle des Betroffenen innerhalb der rechtsextremistischen Organisation herauszustellen. Das Auskunftsersuchen erbrachte den Nachweis dafür, dass der Hauptbetroffene die Transaktionen innerhalb des Personenzusammenschlusses koordiniert und damit letztlich den organisatorischen Zusammenhalt maßgeblich gefördert hat. Ferner erbrachte die Maßnahme Belege für die Existenz sog. „Sektionen“ innerhalb der Organisation. Überdies konnten auf Grundlage der Maßnahme die Mitgliedschaft bereits bekannter Personen nachgewiesen sowie bis dahin noch nicht bekannte Mitglieder identifiziert werden. Unter Würdigung der dargestellten Ergebnisse kann folglich der Nutzen der Maßnahme für die Begründung eines Vereinsverbotsverfahrens

gegen die Organisation durch das Bundesministerium des Inneren im Besonderen hervorgehoben werden.

(3) Fallbeispiel 3 (BfV)

Im Rahmen der Finanzermittlungen zum Hauptbetroffenen konnten diverse auffällige Überweisungen in ein Nachbarland Deutschlands vom BfV festgestellt werden. Zum einen dienten diese der Unterstützung eines dort inhaftierten islamistischen Gefangenen, zum anderen der mutmaßlichen Unterstützung zumindest eines Jihad-Reisenden. So konnte ein Geldtransfer über Western Union an eine Person festgestellt werden, die sich dem „Islamischen Staat“ (IS) angeschlossen hat und während Kampfhandlungen auf Seiten des IS verstorben sein soll. Durch Freigabe der Information durch den ausländischen Partnerdienst hinsichtlich des Geldempfängers und dessen Anschluss an den IS konnten diese Erkenntnisse den Strafverfolgungsbehörden in Form eines Behördenzeugnisses zur Prüfung der Einleitung eines Ermittlungsverfahrens (gemäß § 89c StGB) übermittelt werden.

(4) Fallbeispiel 4 (BfV)

Durch das Auskunftsersuchen konnte die finanzielle Unterstützung einer Person, die sich in Syrien aufhielt, durch deren in Deutschland lebende Familie festgestellt bzw. nachgewiesen werden. Darüber hinaus wurden Kontakt- bzw. Mittelsmänner bekannt, die – möglicherweise über diesen Fall hinaus – eine Rolle bei der finanziellen Unterstützung von Deutschland aus an in Syrien aufhältige Personen spielen. Im weiteren Verlauf konnten neue nachrichtendienstliche Ermittlungsansätze generiert werden.

9.1.2. Fallbeispiele zu § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG

(1) Fallbeispiel 1 (BfV)

Das Auskunftsersuchen des BfV richtete sich gegen Personen, die verdächtigt wurden, der islamistisch-terroristischen Organisation IS anzugehören und deren Aktivitäten i. S. d. §§ 129 a und b StGB von Deutschland und vom Ausland aus zu unterstützen. Die Personen sollen sich in Deutschland bzw. benachbarten Staaten aufgehalten haben und im Kontakt mit einem bekannten Unterstützer des „Islamischen Staates“ gestanden haben. Durch die Maßnahme konnten Erkenntnisse zu möglichen Kontaktpersonen gewonnen werden, die zur Einleitung von Ermittlungen dienten und zur Identifizierung einzelner Betroffener beitrugen.

(2) Fallbeispiel 2 (BfV)

Das Auskunftsersuchen des BfV richtete sich gegen eine Person, die verdächtigt wurde, als Mitglied und Unterstützer der islamistisch-terroristischen Organisation „al-Qaida“ an der Durchführung eines Anschlages in Europa beteiligt zu sein. Durch die Maßnahme konnten Daten zu ausländischen Kontaktrufnummern der Person während eines kurzzeitigen Deutschlandaufenthaltes gewonnen werden. Diese Daten wurden dem BND und mehreren ausländischen Nachrichtendiensten zur Verfügung gestellt, um weitergehende Maßnahmen gegen die Person in dessen Heimatland zu ermöglichen.

(3) Fallbeispiel 3 (BfV)

Das Auskunftsersuchen des BfV richtete sich gegen eine Person, die enge Kontakte zur Führungsebene des IS unterhielt bzw. weiterhin unterhält. Auf Grundlage dieser Informationen konnten verschiedene aufeinander aufbauende Maßnahmen eingeleitet werden, die letztlich die aktuelle Rufnummer zu Tage förderten. Mit Hilfe der übermittelten Daten konnte der Aufenthaltsort des zunächst nicht identifizierten Betroffenen in Deutschland weiter eingegrenzt werden. Im weiteren Verlauf konnten neue nachrichtendienstliche Ermittlungsansätze generiert werden.

(4) Fallbeispiel 4 (BfV)

Das Auskunftsersuchen des BfV richtete sich gegen eine in Deutschland wohnhafte Person, die verdächtigt wurde, der islamistisch-terroristischen Organisation IS anzugehören und deren Aktivitäten von Deutschland aus zu unterstützen. Die Maßnahme führte zur Aufdeckung von bislang unbekannten, in der Vergangenheit liegenden Kontakten der Person in Deutschland und im Ausland. Zur weiteren Aufklärung dieser Kontakte wurden Behördenermittlungen eingeleitet und Erkenntnisanfragen an andere Dienste gestellt.

9.2. Konkrete Fallbeispiele für den Einsatz des IMSI-Catchers

(1) Fallbeispiel 1 (BfV)

Zu einem in Deutschland mit Aufenthaltstitel wohnenden Ausländer lagen tatsächliche Anhaltspunkte vor, dass er eine ausländische terroristische Vereinigung unterstützte und eine bestimmte Mobilfunknummer zur Kommunikation mit potenziellen Attentätern nutzen sollte. Die Person hatte keine Telefonnummern bei Netzanbietern registriert. Eine Observationsmaßnahme zeigte, dass die Person im persönlichen Kontakt mit einem einschlägig bekannten Personenkreis stand. Es ließ sich zudem beobachten, dass die Person in der Öffentlichkeit mit verschiedenen Mobilfunktelefonen hantierte. Erst durch mehrfachen Einsatz eines IMSI-Catchers ließen sich der Zielperson weitere Rufnummern zuordnen. Dies ermöglichte weitere operative Maßnahmen.

(2) Fallbeispiel 2 (BfV)

Der Einsatz des IMSI-Catchers richtete sich gegen eine Person, die verdächtigt wurde, sich im Auftrag des IS in Deutschland aufzuhalten, um einen Anschlag zu begehen bzw. vorzubereiten. Die Maßnahme konnte hilfreiche Aufschlüsse über das Telekommunikationsverhalten der Person geben. Außerdem konnte eine laufende G 10-Maßnahme ergänzt werden, da neue IMEI-Nummern der Person festgestellt werden konnten. Durch die Polizei wurde ein Ermittlungsverfahren bei der zuständigen Staatsanwaltschaft beantragt. Zur Unterstützung polizeilicher Maßnahmen wurden die bekannten IMEI-Nummern übermittelt.

(3) Fallbeispiel 3 (BfV)

Der Einsatz des IMSI-Catchers richtete sich gegen eine Person, die verdächtigt wurde, in Anschlagspläne involviert zu sein. Die Maßnahme wurde notwendig, da davon ausgegangen wurde, dass die Person ein weiteres, bislang unbekanntes Mobiltelefon nutzte. Durch den IMSI-Catcher konnten eine IMSI- und eine IMEI-Nummer festgestellt werden, die der besagten Person zugerechnet werden konnten. Der GBA leitete u. a. auf Grundlage eines Behörden-

zeugnisses des BfV ein Ermittlungsverfahren gegen den Hauptbetroffenen der o. g. Maßnahme gemäß §§ 129 a, b StGB ein. Das LKA wurde mit den Ermittlungen beauftragt, nachdem der Hauptbetroffene vor seinem Wohnobjekt festgenommen wurde. Zwecks Einbeziehung der besagten IMSI- bzw. IMEI-Nummer in die operativen Maßnahmen des LKA wurden diese durch das BfV gerichtsverwertbar übermittelt.

(4) Fallbeispiel 4 (BAMAD)

Der IMSI-Catcher kam zur Informationsbeschaffung im Aufgabenbereich Extremismus/-Terrorismusabwehr bei Ermittlungen des BAMAD zu einem Sachverhalt zum Einsatz, bei dem der konkrete Verdacht bestand, dass Islamisten versuchten, Angehörige der Bundeswehr gezielt für ihre verfassungsfeindlichen Ziele zu instrumentalisieren. Mit der Maßnahme wurden weitere Kontaktpersonen aus dem Umfeld der Szene als mögliche Angreifer festgestellt. Vor dem Hintergrund der durch islamistisch beeinflusste Angehörige des Geschäftsbereichs des BMVg möglicherweise ausgelösten Gefahren wird deutlich, in welchem besonderen Gefahrenumfeld die besonderen evaluierungspflichtigen Befugnisse des BAMAD zum Einsatz kommen.

9.3. Anhang begleitende Erhebung

9.3.1. Begründung für die Nutzenbewertung (BfV, BAMAD und BND) (§ 8a Abs. 2 und 2a BVerfSchG, § 3 BNDG und § 4a MADG)

Bewertung und Begründung	Anzahl
Sehr hoher Nutzen	**5**
Hierbei handelte es sich um eine § 8a-Maßnahme. Diese richtete sich gegen eine Person wegen des Verdachts, schwerwiegende Gefahren für die Sicherheit der Bundesrepublik Deutschland nachdrücklich zu fördern, indem sie für den Geheimdienst einer fremden Macht eine geheimdienstliche Agententätigkeit gegen die Bundesrepublik Deutschland ausübt. Der Nutzen der erhobenen Informationen wird hier für die nachrichtendienstliche Arbeit als sehr hoch bewertet. Durch den Einsatz konnten neue, relevante Informationen gewonnen werden, die in die weitere Bearbeitung einfließen.	1
Die Maßnahme führte zu dem Ergebnis, dass der Hauptbetroffene in Kontakt mit anderen, hier bereits vorab bekannten Kommunikationsmitteln der islamistisch-gewaltbereiten Szene stand. Mittels der Analyse der Geo-Standortdaten konnten anderweitig erlangte Informationen aus dem Umfeld der Hauptbetroffenen teilweise falsifiziert werden. Die Maßnahme war vor allem anfangs unverzichtbar für die Aufklärung des Gefährdungspotenzials des Hauptbetroffenen.	1
Im Zusammenhang mit anderen Ermittlungsergebnissen in dem Sachverhalt konnten tatsächliche Anhaltspunkte für den bestehenden Verdacht untermauert wurden.	1
Mittels der erhobenen Daten und im Kontext derer zu anderen nachrichtendienstlichen Informationen konnten die der Antragstellung zugrunde liegenden tatsächlichen Anhaltspunkte für den Verdacht der Spionagetätigkeit erhärtet werden.	1
Tatsächliche Anhaltspunkte für den bestehenden Verdacht konnten durch die Datenauswertung bestätigt werden.	1
Hoher Nutzen	**18**
Aufstellung der Kontakthäufigkeiten zwischen den Nutzern inkl. deren Geolokalisation	1
Aus den Verbindungsdaten der Maßnahme konnte festgestellt werden, dass der Hauptbetroffene aktuell Kontakt zu einem Funktionär der "Hizb Allah" hat. Der Verantwortliche aus dem Libanon hatte gemäß eines AND im Jahr 2013 den HB für die Organisation rekrutiert. Aus der Auswertung der Verbindungsdaten über TK-DAS ging zudem hervor, dass der HB im Überwachungszeitraum unterschiedliche Mobilfunkgeräte genutzt und zwischenzeitlich die entsprechenden SIM-Karten gegeneinander aus- und wieder zurückgetauscht hat. Dies spricht neben weiteren Erkenntnissen zur Person für ein konspiratives Verhalten des HB.	1

Das anvisierte Ziel der Maßnahme wurde vollumfänglich erreicht. Hier insbesondere durch die Aufbereitung der erhobenen Daten. Es konnten weitere relevante Verbindungen des Hauptbetroffenen aufgedeckt werden, bzw. konnte durch die Maßnahme entlastendes Material gewonnen werden.	1
Der Anfangsverdacht konnte bestätigt werden.	1
Der Verdacht konnte nicht erhärtet werden.	1
Die angefallenen Daten bestätigten die Nutzung dieser Nummer durch den Hauptbetroffenen.	1
Die Maßnahme ergab einen Ansatz für weitere Ermittlungen.	1
Die Stammdatenauskunft ergab Hinweise auf eine Vielzahl weiterer Konten, deren Daten in einem Folgeantrag bei den jeweiligen Kreditinstituten abgerufen wurden. Die Auskünfte hierzu stehen noch aus.	1
Durch die Maßnahme konnte eine IMEI-Nummer der überwachten Mobilfunknummer ermittelt werden, die sonst nicht bekannt geworden wäre.	1
Durch die Maßnahme konnten in- und ausländische Kontaktnummern der Zielperson festgestellt werden. Die Maßnahme wurde parallel zur G10-Maßnahme gegen die Zielperson durchgeführt und ergänzt die daraus gewonnenen Erkenntnisse.	1
Durch die Maßnahme konnten weitere Ermittlungsansätze generiert werden. Diese sind als "hoch" zu bewerten, selbst wenn diese Ermittlungen im Ergebnis zu keinen belastbaren Ergebnissen geführt haben.	1
Durch die Maßnahme konnten zahlreiche weitere Erkenntnisse zur Einholung und Auswertung des zugrundeliegenden Sachverhaltes gewonnen werden.	1
Durch die Maßnahme wurden neu relevante Kontaktdaten bekannt, die weitere Ermittlungsansätze bilden.	1
Erkenntnisse bestätigten sich und Erkenntnisgewinn	1
Fachabteilung kann diese Informationen zwecks Gesamtschau des Sachverhalts weiter in die Fallbearbeitung einfließen lassen.	1
Im Rahmen der Auswertung der Verkehrsdaten konnten nachrichtendienstlich relevante Hinweise über Aufenthaltsorte der Betroffenen sowie Kontaktumfeldes gewonnen werden.	1
Weitere Maßnahmen wurden eingeleitet.	1
Wertvolle Hinweise zum Kontaktfeld der Zielpersonen, Ansatzpunkte für Ermittlungen zu Kontaktpersonen, Hinweise auf Aktivitäten der Zielpersonen durch Auswertung der Standortdaten	1
Teilweise von Nutzen	**12**
Die bisherigen Erkenntnisse konnten nicht klar bestätigt werden.	1

Die Daten gaben keinen unmittelbaren Hinweis für die nachrichten-dienstliche Involvierung. Gleichwohl konnten Hinweise auf Kontakte des Hauptbetroffenen gewonnen werden.	1
Die Informationen waren geeignet, eine Beteiligung anderer Personen auszuschließen und den Betroffenen aufzuklären.	1
Die Stammdatenauskunft ergab Hinweise auf eine Vielzahl von Konten, deren Daten in einem Folgeantrag angerufen wurden. Schon nach der Stammdatenauskunft gab es Hinweise, dass nicht alle Konten dem Betroffenen zuzuordnen waren, sondern es sich um einen Namens (Geburtstags-) Vetter handeln dürfte. Erst der Abgleich über die Wohn-anschrift des Betroffenen mit den beiden angeschriebenen Banken vorhandenen Daten brachte Klarheit.	1
Inhaltsdaten würden weiteren Aufschluss über die Art des Kontaktes geben.	1
Kann hier nicht eindeutig bewertet werden	2
Mittels der Maßnahme konnte das Kontaktumfeld weiter konkretisiert werden. Allerdings ist die Differenzierung zwischen Kontakten des Hauptbetroffenen und der Nebenbetroffenen aufwendig.	1
Parallel wurde eine G 10-Maßnahme durchgeführt.	3
Vollständige Zulieferung seitens des Providers, allerdings konnten durch diese Maßnahme allein noch keine erhärtenden Erkenntnisse gewonnen werden. Gleichwohl konnte ein umfangreicher Einblick in das (über telefonische Verbindungen) aufgebaute Kontaktumfeld des Betroffenen gewonnen werden.	1
Geringer Nutzen	**4**
Durch die Maßnahme konnten keine weiterführenden Informationen zu relevanten Personen im Kontaktfeld des Betroffenen gewonnen werden.	1
Es konnten keine relevanten Kontakte festgestellt werden, gleichwohl konnten durch die Maßnahme Indizien auf das Umfeld des betroffenen gewonnen werden.	1
Kaum Erkenntnisgewinn aufgrund geringer Umsätze auf dem Konto	1
Kaum Rückläufe durch den Provider ans BfV.	1
Sehr geringer Nutzen	**2**
Einschlägige Verbindungsdaten im Sinne des Anfangsverdachtes konnten nicht gewonnen werden.	1
Es konnten durch die Maßnahme keine weiteren Erkenntnisse gewonnen werden.	1
Keine abschließende Bewertung möglich	**14**
Auswertung liegt dem Fachbereich noch nicht vollständig vor.	1
Bei den Providern fielen keine relevanten Daten an.	1

Die Auswertung der Daten dauert an. Ggf. schließen sich weitere Maßnahmen an.	1
Die Auswertung der Daten dauert noch an.	3
Die Finanzermittlung ist noch nicht abgeschlossen. Daher kann noch keine Aussage zum Nutzen getroffen werden. Erst nach abschließender Auswertung der Finanzdaten und anschließender Einordnung und Auswertung der Informationen im Gesamtzusammenhang des Falls durch den Fachbereich ist eine Aussage darüber möglich.	2
In durchgeführten Zeitraum konnten keine relevanten nachrichtendienstlichen Informationen erhoben werden.	1
Kaum Nutzen, da Betroffener äußerst konspirativ.	1
Nach so kurzer Frist kann noch keine Aussage zum Nutzen der Frist getroffen werden. Erst nach abschließender Auswertung der Finanzdaten und anschließender Einordnung und Auswertung der Informationen im Gesamtzusammenhang des Falls durch den Fachbereich ist eine Aussage darüber möglich. Daher wird hierzu zum 15.12.2017 nachberichtet.[249]	4

9.3.2. Begründung für die Nutzenbewertung (BfV und BAMAD) (§ 17 Abs. 3 BVerfSchG)

Bewertung und Begründung	**Anzahl**
Sehr hoher Nutzen	**17**
Aufgrund mehrerer Treffermeldungen konnten zahlreiche Erkenntnisse zur Person gewonnen werden.	1
Aufgrund mehrerer Treffermeldungen konnten zahleiche Erkenntnisse zur Person gewonnenen werden. Insbesondere wurde die Ersteinreise der Person nach Deutschland festgestellt.	1
Der Zweck der Maßnahme wurde erreicht. Wertige Erkenntnisse zur Zielperson konnten gewonnen werden.	1
Die Ausreise konnte festgestellt werden.	1
Die Person ist zurückgekehrt.	1
Die Person konnte bei er Wiedereinreise festgestellt werden.	1
Die Person konnte mehrfach angetroffen werden. Hierdurch wurden relevante Erkenntnisse zur Person bekannt.	1
Die Person konnte zwar nicht angetroffen werden, jedoch wurde dadurch der Aufenthalt der Person im Schengen-Gebiet mit einiger Wahrscheinlichkeit ausgeschlossen.	1
Die Rückkehr/Wiedereinreise der betroffenen Person konnte festgestellt werden.	1
Die SIS-Treffermeldungen dienten zur Aufklärung des Sachverhaltes.	2

[249] Eine nachträgliche Berichterstattung ist bis zur Abgabe des Abschlussberichts nicht erfolgt.

Die Wiedereinreise konnte festgestellt werden.	1
Es konnte die Aus- Wiedereinreise festgestellt werden.	2
Nur mit Hilfe der Ausschreibung wird das BfV über relevante Treffermeldungen direkt informiert. Besonders im Fall von Syrien-Rückkehrern ginge sonst eine erhöhte Gefährdung von einer unbemerkten oder verspätet bemerkten Einreise der ausgeschriebenen Person aus.	1
Person war im Verdacht, Reisetätigkeiten zur Schleusung von Personen aus dem islamistischen Spektrum durchzuführen bzw. selbst die Absicht zu haben, in Jihad-Gebiete zu reisen. Stützende Erkenntnisse für diesen Verdacht konnten durch die Ausschreibung gewonnen werden. Die Weiterreise der Person wurde verhindert.	1
Person wurde nicht angetroffen.	1
Hoher Nutzen	**68**
Anhand der Ausschreibung konnte die Wiedereinreise nach Deutschland und die daraufhin erfolgte Festnahme festgestellt werden.	1
Da keine Beobachtung im virtuellen Raum mehr erfolgen konnte, boten die Treffermeldungen Hinweise über Aufenthaltsort, Begleitperson und z. T. Aktivitäten. Auch die Information, dass keine Ausreise erfolgte, ist wertvoll.	1
Das Kfz wurde mehrfach erfasst und im Zuge der ausschreibebedingten Kontrollen konnte mehrere Nutzen festgestellt werden, die wiederum Rückschlüsse auf weitere Kontaktpersonen zuließen.	1
Der Jihadist wurde Anfang 2016 ausgewiesen und kam nicht mehr zurück.	1
Die ausgeschriebene Person wurde angetroffen und in ihr Herkunftsland zurückgeschoben.	1
Die Ausschreibung konnte einen Beitrag zum Hintergrund von Reisen leisten. Zum Teil wurden diese Reisen überhaupt erst durch die Ausschreibung bekannt.	1
Die Ausschreibung wurde als zusätzliche Informationsquelle zur Lokalisierung sowie Einschätzung des Gefährdungspotenzials der ausgeschriebenen Person genutzt. Durch die Ausschreibung konnte festgestellt werden, dass die Reisebewegungen lediglich einen familiären Hintergrund hatten und keine Bezüge zu möglichen terroristischen Aktivitäten hatten.	3
Die Einreise der Person wurde über eine SIS-Treffermeldung festgestellt.	1
Die Informationen enthielten hier bislang unbekannte Angaben zu Reisebewegungen und Kontaktpersonen.	1
Die Informationen enthielten hier bislang unbekannte und sehr umfangreiche Angaben zu Reisebewegungen und Kontaktpersonen.	1
Die Informationen enthielten hier bislang unbekannte und sehr umfangreiche Angaben zu Reisebewegungen.	1

Die Informationen zu einem erhöhten Reiseaufkommen der ausgeschriebenen Person konnten bestätigt werden.	1
Die Person ist wieder eingereist.	1
Die Person konnte einmal angetroffen werden, hierdurch wurden relevante Erkenntnisse zur Kontaktperson bekannt.	1
Die Person konnte festgenommen werden.	1
Die Person reiste sehr wahrscheinlich nicht mehr aus Deutschland aus. Sie hielt sich kurzfristig in Syrien auf.	1
Die SIS-Treffermeldungen dienten zur Aufklärung des Sachverhaltes.	4
Die SIS-Treffermeldungen dienten zur Aufklärung des Sachverhaltes. Insbesondere konnten eine Rückkehr der Person nach Deutschland festgestellt werden.	1
Die Tatsache, dass die Person nicht reiste, war von hoher Relevanz.	1
Die tatsächliche Ausreise und Wiedereinreisen konnten festgestellt werden.	1
Die Treffermeldungen gaben aufschlussreiche Hinweise über Verfassung des Betroffenen, Aufenthaltsort, Begleitpersonen und z. T. Aktivitäten.	1
Die Wiedereinreise und der Aufenthalt im Ausland konnten belegt werden.	1
Die Zielperson konnte bei ihrer Einreise nach Deutschland mit Pyrotechnik festgestellt werden. Die gefährlichen Gegenstände konnten sichergestellt und Strafanzeigen wegen des Verstoßes gegen das Waffen- und SprengstoffG gefertigt werden. Der GBA leitete einen Beobachtungsvorgang ein.	1
Durch das Ergebnis der Kontrolle konnte der Anfangsverdacht falsifiziert werden.	1
Durch die mehrfachen Treffermeldungen konnte festgestellt werden, dass die Person eine Ausreise aus Deutschland plant. Die Ausreiseplanungen wurden als Anknüpfungspunkt für eine Befragung seiner Person genutzt. Bei dem Gespräch entstand der Eindruck, dass von der Person keine Gefahr mehr ausgehe und eine Ausreise zu gestatten sei.	1
Durch die neu gewonnenen Informationen konnten neue nachrichtendienstliche Erkenntnisse generiert werden, was zu einer Verdichtung des Lagebildes genutzt werden konnte.	1
Durch die Treffermeldungen von Sirene Ungarn konnten u. a. Reisezeiträume, -routen und Kontaktpersonen festgestellt werden.	1
Einreiseverweigerung mitgeteilt, relevant für weitere Bearbeitung	1
Es konnten Informationen bestätigt werden, wonach die ausgeschriebene Person einreisen sollte.	1
Es konnten Informationen zu Kontaktpersonen gewonnen werden.	1

Es konnten Informationen zu Reisebewegungen und zur Gewaltbereitschaft der ausgeschriebenen Person festgestellt werden.	1
Es konnten Informationen zur Person selbst sowie zu ihrer Reisetätigkeit gewonnen werden.	1
Es konnten regelmäßig Erkenntnisse zum Aufenthaltsort der Person gewonnen werden und zumindest Teile seiner Reiseroute nachvollzogen werden.	1
Es konnten relevante Informationen über die Entwicklungstendenzen der Person gewonnen werden.	1
Es konnten viele Erkenntnisse dahingehend gewonnen werden, zu welchen Drittländern der Ausgeschriebene Verbindungen hat.	2
Es stand zu befürchten, die ausgeschriebene Person könne nach Syrien ausreisen, um sich dem bewaffneten Jihad anzuschließen. Die Maßnahme diente der Dokumentation der Reisebewegungen der Person.	1
Es stand zu befürchten, die ausgeschriebene Person könne nach Syrien ausreisen, um sich dem bewaffneten Jihad anzuschließen. Ein solcher Ausreiseversuch konnte durch die Ausschreibung festgestellt und verhindert werden. Dennoch gelang die Ausreise, vermutlich auf dem Landweg.	1
Es wurde bekannt, dass der Betroffene Anmelder von Islam-Infoständen in Wolfsburg und Gifhorn ist. Weitere Kontaktpersonen wurden erfolgreich identifiziert.	1
Es wurde festgestellt, dass die Zielperson aus Deutschland ausreiste.	1
Es wurde festgestellt, dass die Zielperson die Einreise in den Schengen-Raum im Beobachtungszeitraum weitestgehend gemieden hat.	1
Es wurde festgestellt, dass sich die Zielperson regelmäßig in Deutschland, aber auch ins Ausland bewegte. Relevante Erkenntnisse mit Bezug zum Jihadismus waren jedoch zuletzt nicht mehr feststellbar.	1
Hinweise auf Ausreiseabsicht bestätigt, Rückkehr festgestellt	1
Maßnahme diente der Feststellung einer wahrscheinlichen Ausreise einer Person, welche jedoch unterblieb.	3
Mögliche Islamismusbezüge, insbesondere die gemutmaßte Ausreise nach Syrien konnte nicht bestätigt werden, weshalb die Voraussetzungen damit auch wegfallen.	1
Notwendig, jedoch aufgrund des Todes in dem Fall nicht zielführend (keine Rückreise).	1
Person konnte wiederholt im SIS-Verbund angetroffen werden. Die Treffermeldungen halfen, ein umfassendes Bild von der Person zu erstellen.	1
Person reiste sehr wahrscheinlich nicht nach Deutschland ein. Dies war wichtig zu wissen, wegen der von ihr ausgehenden Gefährdung.	1

Person wurde angetroffen. Die gewonnenen Erkenntnisse zu Reiseroute, Mitreisenden und mitgeführten Gegenständen sind zur Bewertung des Ausschreibungsziels erforderlich.	1
Person wurde einige Male angetroffen. Informationen waren durchaus wertig, Aufenthalte im Ausland konnten gut nachvollzogen werden.	1
Reisebewegungen, Kontaktpersonen	1
Reiseweg der Person konnte nachvollzogen werden.	1
Relevante Reise dokumentiert und dadurch festgestellt, wer am Jihad-Schauplatz verblieben sein könnte. Einstellung der Maßnahme, da zwischenzeitlich Inhaftierung.	1
Relevante Reise konnte dokumentiert und dadurch festgestellt werden, wer am Jihad-Schauplatz verblieben sein könnte. Einstellung der Maßnahme, da zwischenzeitlich Inhaftierung.	2
Relevante Reisebewegung mit vermutlicher Verbringung von Rekruten nach Syrien durch Zielperson.	1
Rückkehr aus Türkei bzw. Syrien	1
Verdacht gegen Person (Islamismus) konnte ausgeschlossen werden.	1
Wenige Treffermeldungen, aber mit besonderer Relevanz, weil eine Reise nach Russland bekannt wurde. Diese Information konnte anders nicht erhoben werden.	1
Durch die erfolgreiche Maßnahme ergaben sich weitere zielführende Handlungsmöglichkeiten in der Operation. Die VdP konnte nach Kenntnis der Ausreise durch Bundeswehr-eigene Maßnahmen vor der Durchführung von Kampftätigkeiten im Aufenthaltsland wieder nach Deutschland geholt werden.	1
Zu der Person konnte aufgrund mehrerer Treffer der SIS-Ausschreibung sowie von Treffermeldungen der nationalen nachrichtendienstlichen Beobachtung ein aussagekräftiges Bewegungsprofil erstellt werden. Zufällig erfolgte eine zollrechtliche Kontrolle, während derer eine erhebliche Geldmenge aufgefunden wurde. Diese erhärtete den gegen die Person gerichteten Verdacht zunächst zusätzlich. Im Rahmen des koordinierten Vorgehens von Zollkriminalamt, Schweizerischem Nachrichtendienst und BfV konnte der gegen die Person gerichtete Verdacht jedoch schlussendlich ausgeräumt werden.	1
Teilweise von Nutzen	**115**
Antreffmeldung erfolgte erst in Deutschland	1
Antreffmeldung erfolgt erst in Deutschland bei Einreise über Flughafen.	1
Aufenthaltsort der Person wurde bekannt, Erkenntnisse zum Sachverhalt konnten jedoch nicht gewonnen werden.	2
Aufenthaltsort und Kontaktperson konnten festgestellt werden, wobei sich jedoch keine relevanten Erkenntnisse ergaben.	2

Aufgrund einer bestehenden Grenzfahndungsausschreibung wäre ein Transit über Deutschland auch ohne eine SIS-Ausschreibung bemerkt worden. Die Notwendigkeit einer SIS-Ausschreibung entfiel somit.	1
Aufgrund eines bestehenden staatsanwaltschaftlichen Ermittlungsverfahrens wurde die hiesige Ausschreibung zugunsten derjenigen der zuständigen StA zurückgestellt.	1
Aus anderem Aufkommen lagen Hinweise auf Reisen außerhalb des Schengen-Raumes vor. Die Tatsache, dass keine Treffermeldungen eingingen, legte den Verdacht auf die Verwendung hier nicht bekannter Falschpersonalien nahe.	1
Ausschreibungsgrund war der Verdacht gegen den Betroffenen als Schleuser islamistischer extremistischer Nordkaukasier zu fungieren. Die Maßnahme erbrachte zwar Feststellungen der Person und damit verbunden Kontaktpersonen, jedoch keine weiteren Hinweise, um den Ausschreibungsgrund zu bestätigen.	1
Ausschreibungsgrund war die Nutzung des Fahrzeugs bei potenziellen Schleusungsaktivitäten durch einen Nordkaukasier. Die Maßnahme erbrachte zwar Feststellungen des Fahrzeugs und damit verbunden Fahrzeugnutzer, jedoch keine weiteren Hinweise um den Ausschreibungsgrund gegen das Fahrzeug, den Halter und die Nutzer zu aufrechtzuerhalten.	1
Bewegungsbild fallunabhängig von Interesse	1
Da aufgrund des Ausgangssachverhaltes von einem Ausreisewillen des Betroffenen auszugehen war, hatte die Information, dass KEINE Reisebewegung stattfand, auch einen Wert. Jedoch gab es darüber hinaus auch keinerlei Treffermeldungen, die Hinweise über Aufenthaltsort, Begleitpersonen und z.T. Aktivitäten geben konnten.	1
Da die Person nicht angetroffen wurde, konnte zumindest davon ausgegangen werden, dass sie nach ihrer Ausweisung keine Einreiseversuche nach Deutschland/ins Schengen-Gebiet unternommen hat.	1
Da keine Reisebewegung festgestellt wurde, kann zumindest festgehalten werden, dass die Person nicht über Deutschland in ihr Heimatland zurückgereist ist.	1
Da keine Treffermeldung generiert wurde, konnte mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass die Person sich dauerhaft in Deutschland aufhielt.	1
Dass die Person nicht angetroffen wurde, konnte zumindest davon ausgegangen werden, dass sie sich dauerhaft in Deutschland aufhielt.	1
Das Fahrzeug wurde anscheinend als ein "Springerfahrzeug" verwendet. Der zuerst bekannte gewordene Nutzer hat es anschließend nicht wieder genutzt. Es wurden zwar andere Nutzer festgestellt. Diese haben jedoch keinerlei Bezug zum zuerst genannten Nutzer.	1

Der Aufenthaltsort der Person konnte durch die Ausschreibung zwar festgestellt werden, jedoch war der Umfang der Mitteilung von SIRENE Spanien sehr gering.	1
Der Betroffene reiste unter Nutzung gestohlener Ausweispapiere aus, sodass die Ausschreibung ins Leere gelaufen ist; sie konnte jedoch aufgrund der Ausschreibung ihres mitreisenden Lebensgefährten festgestellt werden. Wäre sie mit den richtigen Personalien gereist, wäre für die Betroffene ebenfalls eine Meldung der jeweiligen Behörden (Italien, Griechenland) erfolgt.	1
Der in Rede stehende Verdacht konnte durch die Maßnahme nicht verifiziert, jedoch auch nicht falsifiziert werden.	1
Der Nutzen kann im vorliegenden Fall schlecht bewertet werden, da zwar Hinweise auf eine mögliche Einreise der ausgeschriebenen Person vorlagen, diese Einreise letztlich jedoch nicht stattfand. Die Ausschreibung war gleichwohl notwendig, um über eine Einreise rechtzeitig informiert zu werden.	1
Der zu Grunde liegende Anfangsverdacht (dauerhafte Ausreise nach Syrien; Teilnahme "Jihad") konnte falsifiziert werden.	1
Der zu Grunde liegende Anfangsverdacht konnte falsifiziert werden.	1
Die Ausschreibung konnte einen Beitrag zum Hintergrund von Reisen leisten. Zum Teil wurden diese Reisen überhaupt erst durch die Ausschreibung bekannt.	1
Die Informationen aus den Treffermeldungen enthielten weitere Erkenntnisse zur Person und deren Umfeld und trugen damit zu einer besseren Bewertung bei.	1
Die Person hat keine Ausreiseabsicht mehr.	9
Die Person konnte zwar mehrfach angetroffen werden. Jedoch wurden hierdurch nur wenige relevante Erkenntnisse bekannt.	1
Die Person reiste im Zeitraum der Ausschreibung nur einmal ins Ausland. Zur getätigten Reise konnten relevante Erkenntnisse durch die Ausschreibung gewonnen werden. Aufgrund der geringen Reisetätigkeit der Person sind keine weiteren Erkenntnisse angefallen.	1
Die Person unternahm fast keinerlei Reisen.	1
Durch die Ausschreibung konnte widerlegt werden, dass wie angenommen, die Person sich in Syrien an Kampfhandlungen beteiligt.	1
Durch die Ausschreibungen konnte Erkenntnisse zu den Reisebewegungen und zum Teil auch Hinweise auf Aktivitäten des Ausgeschriebenen gewonnen werden.	1
Durch die Treffermeldung wurde der Aufenthaltsort der Person in Deutschland bekannt.	1

Einerseits erbrachte die Ausschreibung keine Erkenntnisse; dies war andererseits aufgrund der kurzfristigen Einleitung auch nicht unmittelbar zu erwarten. Weiterhin war die Ausschreibung trotz der in der Kürze der Zeit bevorstehenden Abschiebung des Betroffenen für den Fall notwendig, hätte er sich Abschiebung entziehen wollen.	1
Einmaliger Treffer, Gewinnung von Angaben zum Aufenthaltsort der ausgeschriebenen Person	1
Erkenntnis, dass potenzielle AQ-Anhänger aus Belgien Düsseldorf für Reisen nach außerhalb des Schengen-Raumes nutzten.	2
Es bestand ebenfalls eine Ausschreibung gemäß § 17 Abs. 2 BVerfSchG. Mittels dieser konnten die relevanten Reisebewegungen des Betroffenen über deutsche Flughäfen ebenfalls festgestellt werden. Eine SIS-Ausschreibung war daher nicht mehr notwendig.	1
Es besteht keine Ausreiseabsicht mehr.	14
Es gab keine Treffermeldung, die eine Ausreise der Betroffenen anzeigte.	1
Es konnte keine ergänzenden Erkenntnisse zum Ursprungssachverhalt gewonnen werden.	1
Es konnten keine Erkenntnisse gewonnen werden, die den Ausgangs-sachverhalt erhärtet hätten.	2
Es konnten keine Erkenntnisse gewonnen werden, die den Ausgangs-sachverhalt erhärtet oder entkräftet hätten.	1
Es konnten keine Reisebewegungen durch die Ausschreibungen (SIS sowie Grenzfahndung) festgestellt werden.	1
Es liegt keine Ausreiseabsicht mehr vor.	2
Es sind regelmäßige Reisen festgestellt worden. Der Ausgangssachverhalt konnte jedoch nicht näher erhärtet/konkretisiert werden.	1
Es wurde festgestellt, dass sich die Zielperson in Deutschland bewegt. Relevante Erkenntnisse mit Bezug zum Jihadismus waren jedoch zuletzt nicht mehr feststellbar, ebenso wie Auslandsreisen.	1
Es wurde festgestellt, dass sich die Zielperson in Deutschland bewegt hat.	1
Es wurde festgestellt, dass sich die Zielperson in Deutschland bewegt. Relevante Erkenntnisse mit Bezug zum Jihadismus waren jedoch zuletzt nicht mehr feststellbar, ebenso wie Auslandsreisen.	1
Es wurde lediglich eine Treffermeldung am Flughafen Düsseldorf im Rahmen der Ausschreibung zur Grenzfahndung generiert, sodass diese im vorliegenden Fall ausgereicht hätte, da keine Reisen auf dem Landweg o.a. stattfanden.	1
Es wurden keine Treffermeldungen generiert, sodass zumindest mit hoher Wahrscheinlichkeit davon ausgegangen werden konnte, dass sich die Person dauerhaft in Deutschland aufhielt.	1

Es wurden zwar keine Treffermeldungen generiert, sodass keine unmittelbaren Erkenntnisse gewonnen werden konnten. Mittelbar konnte dadurch jedoch mit sehr hoher Wahrscheinlichkeit von einem Aufenthalt in Deutschland ausgegangen werden.	1
Feststellung (unauffälliger) innereuropäischer Reisebewegungen	1
Im Rahmen von Treffermeldungen übermittelte Erkenntnisse waren hier nicht von hoher Relevanz.	1
Keine Auffälligkeiten, insofern auch keine Gewinnung nachrichten-dienstlicher relevanter Informationen.	1
keine besondere Relevanz	2
Kontaktpersonen konnten festgestellt werden, nachrichtendienstlicher Nutzen war allerdings gering, da es sich um keine nachrichtendienstlich relevanten Personen handelte.	1
Lediglich Besuchsreisen zur Familie festgestellt, keine nd-relevanten Zusammenhänge und Erkenntnisse	1
lediglich Feststellungen innerhalb Bayerns	1
Maßnahme diente insbesondere der Absicherung für den Fall der überraschenden Entlassung des Ehemannes aus der U-Haft und einer damit zu erwartende Ausreise des Ehepaares. Da der Ehemann nicht entlassen wurde, ist der Zweck letztlich nur teilweise erfüllt worden. Eigene Reisen der Person waren unauffällig und in der Gesamtschau von untergeordneter Relevanz.	2
Person ist ein salafistischer Prediger. Er ist in Deutschland als solcher grundsätzlich nicht erwünscht. Ein Aufenthalt in Deutschland war aber nicht feststellbar.	1
Person konnte angetroffen werden. Alias-Personalie konnte ermittelt werden, ausländerrechtlich interessant, allerdings keine wertigen nachrichtendienstlichen Erkenntnisse.	2
Person konnte im Ausschreibungszeitraum angetroffen werden. Weiter-führende nachrichtendienstlich relevante Erkenntnisse zur Person konnten nicht generiert werden. Person wird nur noch bedingt in der islamistischen Szene verortet.	1
Person konnte nicht angetroffen werden.	2
Person tätigte nicht die beabsichtigte Reise.	2
Person war nicht im Schengen-Raum aufzufinden. Ggf. war er gar nicht eingereist.	1
Person war zu Ausschreibungsbeginn bereits an einen Jihadschauplatz ausgereist. Im Ausschreibungszeitraum ist er dort bei Kampfhandlungen auf Seiten einer jihadistisch-terroristischen Vereinigung verstorben.	1
Person wurde angetroffen, so wurden Kontaktpersonen bekannt. Vermutlich besteht jedoch kein Extremismusbezug.	1

Person wurde angetroffen. Die gewonnenen Erkenntnisse zu Reiseroute, Mitreisenden und mitgeführten Gegenständen sind zur Bewertung des Ausschreibungsziels erforderlich.	3
Person wurde nicht angetroffen, was für keine große Reisetätigkeit spricht.	1
Person wurde nicht angetroffen.	1
Person wurde nicht angetroffen. Es konnten also keine Informationen gewonnen werden. Allerdings lag das mutmaßlich an der mangelnden (Rück-)Reisetätigkeit.	1
Person wurde nicht angetroffen. Nach dem Versterben der Person waren die Voraussetzungen für die Ausschreibung nicht mehr gegeben.	1
Person wurde nicht im Rahmen der SIS-Ausschreibung angetroffen, sondern im Rahmen einer parallel laufenden Ausschreibung im geschützten Grenzfahndungsbestand der Bundespolizei. Trotz bestehender Ausschreibung gelang der Person mittels eines anderen Ausweisdokumentes der Ausreise in ein Jihadgebiet über einen anderen europäischen Flughafen. Passentziehende Maßnahme sowie Untersuchungshaft waren teilweise im Ausschreibungszeitraum angeordnet gewesen, sodass ein weiteres Antreffen nicht zustande kam.	1
Person wurde nicht im Rahmen der SIS-Ausschreibung angetroffen, sondern lediglich im Rahmen einer nationalen Grenzfahndungs-ausschreibung. Aufgrund bekannter Ausreiseabsichten und eines erfolgten Passentzugs war die Maßnahme dennoch geboten und geeignet, auch die anderen europäischen Grenzbehörden über den Sachverhalt in Kenntnis zu setzen.	1
Person wurde zwar angetroffen, etwaige Islamismusbezüge konnten jedoch nicht genauer verifiziert werden, sodass die Ausschreibung nicht fortgeführt werden konnte.	1
PKW der Zielperson und die Zielperson selbst waren nicht im Schengen-Raum aufzufinden. Ggf. war er gar nicht eingereist.	1
Regelmäßige Ein- und Ausreisen konnten dokumentiert werden. Weitere Ansatzpunkte für weiterführende Maßnahmen ergaben sich jedoch nicht.	1
Reise von Belgien und Frankreich nach Marokko und zurück; Erkenntnis-gewinn, jedoch Hintergründe der Reisen nicht klar und keine Kontaktperson festgestellt.	1
Reisebewegungen konnten festgestellt werden. Es wurden jedoch keine nachrichtendienstlich relevanten Feststellungen gemacht.	1
Reisewege der Person konnten nachvollzogen werden; nachrichten-dienstliche relevante Erkenntnisse wurden nicht erlangt.	1
Umfangreiche Erkenntnismitteilung bei Antreffen der Person, allerdings keine den Anfangsverdacht erhärtende Erkenntnisse	1
Verdacht hat sich nicht bestätigt. Jedoch konnte die Ausschreibung (die Treffer) auch zur Entkräftung des Verdachts beitragen.	1

Zwar konnten keine Reisebewegungen der ausgeschriebenen Person über die Ausschreibung gewonnen werden, jedoch ist daraus immerhin abzuleiten, dass die ausgeschriebene Person entgegen der ursprünglichen Einschätzung keine Rückreise nach Deutschland beabsichtigte.	1
Zwar konnten keine Reisebewegungen der ausgeschriebenen Person über die Ausschreibung gewonnen werden, jedoch ist daraus immerhin abzuleiten, dass die ausgeschriebene Person entgegen der ursprünglichen Einschätzung keine Rückreise nach Deutschland beabsichtigte.	1
Geringer Nutzen	**54**
Ausschreibung einer ausreisewilligen Person mit Ausreiseverbot (konkrete Hinweise auf geplante Ausreise zwecks Jihadteilnahme in Syrien). Ausreise fand im weiteren Verlauf nicht statt. Mittlerweile glaubhafte Abwendung der Person von Ausreiseplänen.	1
Da der Betroffene keine Reiseaktivitäten entfaltete, konnten keine konkretisierenden Erkenntnisse zum Ausgangssachverhalt gewonnen und die Ausschreibung insbesondere im Hinblick auf die Verhältnismäßigkeit nicht weiter fortgeführt werden.	2
Da die Person nicht angetroffen wurde, trug die Ausschreibung nicht zu einer weiterführenden nachrichtendienstlichen Aufklärung bei.	1
Die Person konnte zwar nicht angetroffen werden, jedoch wurde dadurch ein Aufenthalt der Person im Schengen-Gebiet mit einiger Wahrscheinlichkeit ausgeschlossen.	1
Die ausgeschriebene Person wurde nicht angetroffen.	1
Die ausgeschriebene Person wurde im Rahmen der Ausschreibung nicht angetroffen.	1
Die ausgeschriebene Person wurde nicht angetroffen.	1
Die Maßnahme wurde für den Fall beantragt, falls bei bestehendem Ausreiseverbot ein Ausreiseversuch unternommen würde. Die Lebensumstände der Person hatten sich seitdem geändert, so dass ein Antreffen sehr unwahrscheinlich wurde.	1
Die Person bewegte sich innerhalb Deutschlands.	1
Die Person konnte durch die Ausschreibung nicht festgestellt werden, sie wurde aufgrund eines Ermittlungsverfahrens festgenommen.	1
Die Person konnte nicht angetroffen werden, demzufolge auch kein Informationsgewinn.	1
Die Person konnte zwar nicht angetroffen werden, jedoch wurde dadurch ein Aufenthalt der Person im Schengen-Gebiet mit einiger Wahrscheinlichkeit ausgeschlossen.	1
Die Person konnten im Ausschreibungszeitraum nicht angetroffen werden.	1

Die Reisetätigkeiten standen nicht in unmittelbarem Zusammenhang zum Beobachtungsobjekt.	1
Durch die Maßnahme konnten keine Reiseaktivitäten der Person festgestellt werden. Die Person konnte auch nicht weiter in Deutschland lokalisiert werden. Dementsprechend konnten keine weiteren Aufklärungsmaßnahmen durch das BfV veranlasst werden.	6
Es ergaben sich keine Erkenntnisse im Sinne des Anfangsverdachts.	1
Es konnte durch die Maßnahme keine Erkenntnisse gewonnen werden, die eine Reiseaktivität innerhalb des Schengen-Raums belegen konnten, welche allerdings vermutet wurde. Zudem konnten durch die fehlende Reiseaktivität keine Erkenntnisse zu Kontaktpersonen oder aktuellen Erreichbarkeiten oder äußerlichen Besonderheiten gewonnen werden.	1
Es konnte keine Erkenntnisse gewonnen werden, da die Person nicht angetroffen wurde.	1
Es konnten anhand der Ausschreibung im geschützten Grenzfahndungs-bestand zwar Reisen der Person aus Deutschland in außereuropäische Ausland festgestellt werden, aber eine Reise innerhalb des Schengen-Raumes wurde nicht festgestellt. Daher konnten auch keine Erkenntnisse gewonnen werden, die bei einem Antreffen ggf. vorgelegen hätten.	1
Es konnten keine Reisebewegungen der Person festgestellt werden.	1
Es konnten keine relevanten Reisen des Betroffenen festgestellt werden.	1
Es lagen Hinweise darauf vor, dass die Person nach Deutschland reisen will. Eine Reise konnte nicht festgestellt werden.	1
Es sind trotz mehrfacher Verlängerung der Ausschreibung keine relevanten Erkenntnisse angefallen.	1
Es wurde indirekt eine neue Information gewonnen, allerdings ließen sich daraus keine neuen nachrichtendienstlichen Erkenntnisse generieren.	1
Es wurden im Wesentlichen keine neuen Informationen gewonnen. Es konnten zwar keine neuen nachrichtendienstlichen Erkenntnisse generiert werden. Allerdings wurden bereits vorliegende Erkenntnisse bestätigt.	1
Es wurden nur unwesentliche neue Informationen gewonnen. Sie ließen sich allenfalls zur Bestätigung bereits anderweitig gewonnener nachrichtendienstlicher Erkenntnisse nutzen.	1
Im Zeitraum der Maßnahme wurde die ausgeschriebene Person nur in geringem Maße angetroffen. Wertige nachrichtendienstliche Informationen wurden nicht gewonnen.	1
Keine Gewinnung relevanter Erkenntnisse	1
Keine SIS-Treffermeldungen erlangt.	1
Keine Treffermeldung erhalten.	3
Lediglich eine Treffermeldung ohne Relevanz.	1

Person ist nicht im Rahmen der SIS-Ausschreibung angetroffen worden.	1
Person konnte nicht angetroffen werden.	5
Person reiste auf Ankündigung nach Deutschland ein und ließ sich bezüglich Behördenanfragen anwaltlich vertreten.	1
Person wurde nicht angetroffen und hat sich von der Szene entfernt.	1
Person wurde nicht angetroffen, daher kein Erkenntnisgewinn.	1
Person wurde nicht angetroffen, daher keine neuen Erkenntnisse durch die Ausschreibung.	1
Person wurde nicht angetroffen.	4
Zweck nicht erreicht	1
Sehr geringer Nutzen	**60**
Person hat keine Auslandsreisen unternommen, sodass durch die Maßnahme keine Informationen gewonnen werden konnten.	1
Da die Person nicht angetroffen wurde (vgl. Frage 4), wurden durch die Ausschreibung keine Informationen gewonnen, die bewertet werden könnten.	1
Die Person wurde nicht angetroffen.	2
Die ausgeschriebene Person wurde im Rahmen der Ausschreibung nicht angetroffen.	1
Es wurden keine neuen Informationen gewonnen und somit auch keine neuen nachrichtendienstlichen Erkenntnisse generiert werden.	1
Es wurden keine neuen Informationen gewonnen und somit konnten auch keine neuen nachrichtendienstlichen Erkenntnisse generiert werden.	10
Es wurden keine neuen Informationen gewonnen. Somit konnten auch keine nachrichtendienstlichen Erkenntnisse generiert werden.	1
Kein Antreffen der Person	1
Keine Erkenntnisse gewonnen	2
Keine neuen Informationen und somit auch keine neuen Erkenntnisse	1
Keine Treffer	1
Keine Treffermeldung	6
Person ist im Überwachungszeitraum aus Deutschland nach Marokko ausgewandert. Ein SIS-Fahndungstreffer wurde aber nicht erzielt.	1
Person wurde nicht angetroffen.	28
Trotz identischer Personalien stellte sich heraus, dass es sich bei der ausgeschriebenen Person nicht um die gesuchte Person handelt.	1
Zweck der Maßnahme konnte nicht erreicht werden	2

Keine Angabe	**2**
k.A.	1
Die Ausschreibung wurde wegen entfallender Zuständigkeit des MAD aufgrund der Entlassung des Betroffenen aus der Bundeswehr vorzeitig beendet.	1

9.3.3. Begründung für die Nutzenbewertung (§ 18 Abs. 1a BVerfSchG) (nur Länder)

Bewertung und Begründung	**Anzahl**
Hoher Nutzen	**15**
Die Informationen aus dem genannten Hinweis ermöglicht eine umfassendere Lage- und Personenbeurteilung im Rahmen der Auswertung und führt weiter dazu, interne Handlungsabläufe bzgl. konkreter Personen bedarfsgerechter zu planen und durchzuführen.	1
Die Informationen ermöglichen das Speichern verdächtiger Personen.	1
Die Informationserhebung in diesem Fall ist noch nicht abgeschlossen. Es handelt sich um einen Verdachtsfall einer möglichen Terrorismusfinanzierung. Der Ersthinweis kam von einem Mitarbeiter einer Ausländerbehörde.	1
Erkenntnisse im Sinne von § 4 Abs. 1 Nr. 4 und VerfSchG-LSA	3
Erstmalige Erkenntnis über solche Aktivitäten	1
Hinweis auf einen möglichen terroristischen Verdachtsfall. Sachaufklärung dauert noch an.	3
Mit der Übermittlung der Information der Ausländerbehörde konnte ein bisher noch nicht bekannter Islamist identifiziert werden.	1
Ohne die ABH wäre die Information nicht bekannt geworden.	1
Person war vorher im LfV Hessen nicht bekannt. Eine Speicherung erfolgt lediglich deswegen nicht, da der "Hessenbezug" nicht nachhaltig bejaht werden kann. Abschiebung bereits veranlasst.	1
Wertiger Ersthinweis auf einen möglichen Jihadisten	1
Zwar differiert die tatsächliche Wertigkeit der Hinweise stark, dennoch stellen diese eine wertvolle Quelle dar.	1
Teilweise von Nutzen	**19**
Aus dem Sachverhalt ist kein konkreter Extremismusbezug erkennbar.	1
Ausreise eines irregulären Migranten aus Syrien in den Sudan mit möglicher jihadistischen Motivation. Weitere Abklärungen sind eingeleitet.	1
Bei dem Verfasser des Briefs handelt es sich um einen Ausländer, der sich als Vielschreiber hervorgetan hat. Im Ergebnis konnten psychologische Ursachen als Motivation für die Schreiben herausgearbeitet werden.	1
bislang kein Extremismusbezug	1

Der Vorgang wird derzeit noch als Verdachtsfall weiter bearbeitet. Eine abschließende Einschätzung kann noch nicht erfolgen.	1
Es handelte sich um Hinweise zu möglichen Wesensveränderungen begründet durch eine auffällig geänderte religiöse Kleidung/Bartwuchs/Verschleierung.	1
Folgehinweis zu Fall-Nr. 2	1
Hinweis auf einen möglichen terroristischen Verdachtsfall. Sachverhalt hat sich bisher nicht erhärtet.	1
Hinweis auf eine Person, die extremistische Kontakte unterhalten soll. Wahrscheinlich Denunziation im familiären Umfeld.	1
Informationsübermittlung nur mündlich, schriftliche Mitteilung blieb aus	1
Lediglich sehr vager Hinweis ohne konkreten Inhalt	1
Mit der Übermittlung der Information wurde auf eine kleine Gruppe von Personen hingewiesen, die sich zur gemeinsamen Religionsausübung zusammengefunden haben.	1
Nach Abschluss der Ermittlungen weist der Sachverhalt keine Relevanz für die Arbeit der Behörde auf.	1
Nach Bewertung fehlende Ansatzpunkte für Extremismus.	1
Person wurde 2005 in München wegen Unterstützung einer Terrororganisation (AAI) ausgewiesen, reiste aber offenbar bereits 2015 wieder mit neuen Personalien in Bundesgebiet (BW) ein. Er behauptet inzwischen geläutert zu sein. Seine AE ist zwar Anfang 2017 bereits erloschen, trotzdem erhält er derzeit stets Duldungsverlängerungen.	1
Sachverhalt muss erst weiter abgeklärt werden. Eine endgültige Einschätzung ist noch nicht möglich.	1
Schon relevante Aussage, wurde aber durch Polizei nach Absprache der Polizei relativiert	1
Verdacht der Einreise eines aktiven Kämpfers einer mit der verbotenen PKK assoziierten Gruppierung. Weitere Abklärungen sind eingeleitet.	1
Verdachtshinweis auf Einreise eines Tailban-Angehörigen. Die folgende Bearbeitung brachte keine Bestätigung des Verdachts.	1
Geringer Nutzen	**25**
Aus dem Sachverhalt ergeben sich keine Hinweise auf Islamismus/Salafismus.	1
Aus dem Sachverhalt ist kein konkreter Extermismusbezug erkennbar. Ein Flüchtling mit auffälligen Tätowierungen wurde gemeldet.	1
Aus dem Sachverhalt ist kein konkreter Extremismusbezug erkennbar.	1
Aus dem Sachverhalt ist kein konkreter Extremismusbezug mit Bezug auf Deutschland erkennbar.	1
Der Extremismusbezug hat sich nicht bestätigt.	1

Die im Verfassungstreuebogen angegebene Organisation hat keine Bedeutung für die nachrichtendienstliche Arbeit in Bayern.	1
Eher allgemeine muslimische Aussagen	1
Eine ABH teilte mit, dass es sich nach Auskunft des Ausländers selbst bei einem Dokument um einen Ausweis der Taliban handeln würde. Das LKA und der Staatsschutz wurden eingeschaltet.	1
Einzelfallbezogen, Hinweis deutet eher auf gestörte Persönlichkeit	1
Es konnten keine neuen Erkenntnisse gewonnen werden.	1
Es konnten keine tatsächlichen Anhaltspunkte im Sinne des VerfSchG-LSA festgestellt werden.	2
Hinweis auf einen Flüchtling, der mutmaßlich falsche Personalien angegeben hat. Darüber hinaus soll er einen Facebook-Freund haben, der Waffen als Profilbild habe. Es ließ sich kein Extremismusbezug ermitteln.	1
Hinweis auf einen gewalttätigen Schüler. Kein Extremismusbezug erkennbar.	1
kein Extremismusbezug	1
Keine eindeutigen Erkenntnisse im Sinne von § 4 Abs. 1 VerfschG-LSA	2
Keine Erkenntnisse im Sinne von § 4 Abs. 1 Nr. 4 und VerfSchG-LSA	3
Keine Extremismusbezug, Abgabe an Landespolizeipräsidium	1
Nicht verifizierbarer Hinweis auf Mitgliedschaft in terroristischen Vereinigung	1
Sachverhalt hat sich nicht bestätigt	2
unkonkrete Angaben bei der Übermittlung, warum überhaupt übermittelt wird	1
Sehr geringer Nutzen	**20**
Aus den zur Person vorliegenden Informationen ergibt sich nach eingehender Prüfung der vorliegenden Unterlagen kein Islamismusbezug. Ein Bezug zum IS ist nicht ersichtlich. Die Passdokumente wurden nicht in einem IS-dominierten Gebiet ausgestellt. Soweit dies durch die hier vorliegenden Analysen nachvollziehbar ist, handelt es sich um ein von kurdischen Kräften dominiertes Gebiet. Bei der Persona handelt es sich eigenen Angaben zu Folge um einen kurdischen Volkszugehörigen.	1
Aus der Sachverhaltsschilderung sind keine verfassungsrechtsrelevanten Anhaltspunkte/Verdachtsmomente zu entnehmen.	3
Der Hinweis zur Person ließ auch nach Ermittlungen keine extremistischen oder islamistischen Bezüge zu erkennen. Es handelte sich um eine Meldung aufgrund eines "schlechten Gefühls" bei der betroffenen Person.	1
Die Auffälligkeit der Person wird nur an der Kleidung festgemacht. Keine weiteren Auffälligkeiten bekannt.	1
Die Ermittlungen zur Person ergaben keine Anhaltspunkte auf einen Bezug zum IS. Der Hinweis, der dem AfV zuging, deckte sich mit dem polizeilichen Hinweis. Neue relevante Informationen wurden nicht bekannt. Die StA prüft	1

den Vorgang und sah keine Anhaltspunkte für ein strafbares Verhalten (Kriegsverbrechen o.ä.). Eine Speicherung im NADIS bzw. eine weitere Bearbeitung erfolgt seitens des AfV nicht, da die Hinweisbearbeitung zum SV keine Anhaltspunkte/keinen Islamismusbezug erbrachte. Der gesetzliche Auftrag des AfV ist nicht eröffnet.	
Hinweis auf einen afghanischen Flüchtling, der freiwillig nach Afghanistan zurückreisen will. Kein direkter Extremismusbezug erkennbar.	1
Kein Extremismus feststellbar	2
kein Extremismusbezug	2
Kein Extremismusbezug erkennbar	1
keine Anhaltspunkte auf islamistische Bestrebungen	1
Keine Erkenntnisse im Sinne von § 4 Abs. 1 Nr. 4 und VerfSchG-LSA	3
Keine Relevanz für unsere Arbeit	1
Sachverhalt war bereits über anderen Informationsweg bekannt	1
sehr pauschale Anschuldigung (optische Veränderung, die nicht feststellbar ist)	1
Keine abschließende Einschätzung möglich	**25**
Alle drei übermittelten Personen sind NADIS negativ.	1
Aufgrund der laufenden Ermittlungen und des noch nicht bestätigten Hinweises auf eine Zugehörigkeit zum IS ist eine abschließende Bewertung derzeit nicht möglich	1
Ausgangshinweis kann noch nicht hinreichend bewertet werden, da Vergleichsinformationen fehlen.	1
Bislang nur vager Anfangsverdacht auf extremistischen Hintergrund. Klärung des Sachverhaltes bedarf weiterer Ermittlungen.	4
Der Kontakt der Ausländerbehörde zu Ausländer war abgebrochen, Aufenthaltsort nicht bekannt. Der Ausländer war hier bislang nicht bekannt. Der Vorgang ist nicht nachprüfbar.	1
Der Sachverhalt wurde bisher nicht weiter verifiziert. Die Bearbeitung ist noch nicht abgeschlossen, da die Ermittlungen noch andauern bzw. noch kein Ergebnis vorliegt.	1
Die Ausländerbehörde teilte mit, dass der Ausländer im Rahmen der Sicherheitsbefragung angab, in den letzten drei Jahren nicht in Tunesien gewesen zu sein, obwohl im Reisepass eine Ein- und Ausreise dokumentiert ist. Der Vorgang ist hier nicht nachprüfbar.	1
Die Ermittlungen des BayLfV sind noch nicht abgeschlossen.	1
Die Ermittlungen zur Person laufen noch. Bisher ist nicht zu bestätigen, dass es sich bei der Person um eine extremistische oder islamistische Person handelt. Die Verhaltensauffälligkeiten sind allesamt ohne Religionseinfluss oder Bezüge zur Religion aufgetreten.	1

Er wurde dem AfV wegen seiner islamistischen und aggressiven Äußerungen als potenzieller Gefährder gemeldet. U. a. habe er am 24.03.2017 damit gedroht, den „Führer des IS -AL BAGDADI- her zu holen, damit alle geschlachtet werden“. Er tritt sehr aggressiv gegenüber verschiedenen öffentlichen Stellen auf. Gleichzeitig vermittelt er einen sehr religiösen Eindruck, da er stets einen Koran und seinen Gebetsteppich bei sich trägt. Die ABH schätzt ihn als gefährlich ein, da er wohl nichts mehr zu verlieren habe. Er hätte bereits eine 14-Jährige sexuell belästigt und sei psychisch auffällig.	1
Es wurden auf konspirativem Weg einem Bewohner einer Gemeinschaftsunterkunft für Asylbewerber hohe Gelbeträge von unbekannter Seite zugewiesen, ein Selbstverbrauch des Geldes auszuschließen. Die Ermittlungen dauern hierzu an.	1
Gefälschte Pässe bei Flüchtlingen sind ein Massenphänomen. Dies ist in erster Linie ein polizeiliches/strafrechtliches Problem.	1
Initiativübermittlungen von Ausländerbehörden an das LfV Nordrhein-Westfalen gemäß § 18 Abs. 1a) BVerfSchG werden weder in der Eingangssachbearbeitung noch in der hier geführten Amtsdatei gesondert erfasst. Insofern ist eine konkrete Aussage zur Anzahl der Initiativübermittlungen oder zu daraus resultierenden Speicherungen nicht möglich. Zudem erhält das LfV NRW sowohl im Rahmen von Verfahren zur Personenüberprüfungen als auch im Rahmen der Beteiligung an der Sicherheitskonferenz Nordrhein-Westfalen Informationen aus den Ausländerbehörden.	1
Kein Hinweis auf extremistische Gesinnung. Allgemeine Kriminalität.	1
laufende Bearbeitung	1
laufende Prüfung	1
Person soll bereits ausgereist sein	1
Personenhinweis, noch keine abschließende Einschätzung möglich	2
Sachverhalt befindet sich noch in der Abklärung.	2
Teilweise unbekannte Aufenthalte im Ausland sind nicht nachprüfbar!	1