Deutscher Bundestag
Wissenschaftliche Dienste

Ausarbeitung

Nachrichtendienstliche Befugnisse im Ländervergleich

Nachrichtendienstliche Befugnisse im Ländervergleich

Aktenzeichen:	WD 3 - 3000 - 130/23
Abschluss der Arbeit:	21.12.2023 (zugleich letzter Abruf der Internetseiten)
Fachbereich:	WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Überblick

Die vorliegende Ausarbeitung beschäftigt sich mit den Rechtsgrundlagen für die Beschaffung von Informationen und Übermittlung von Erkenntnissen durch Nachrichtendienste in Deutschland, den Vereinigten Staaten von Amerika (USA), dem Vereinigten Königreich (UK), Frankreich, den Niederlanden und Finnland.

Ziel aller Nachrichtendienste ist es, Informationen zu beschaffen, zu verarbeiten, unter Umständen auch an andere Stellen weiter zu übermitteln, um insbesondere die jeweilige Regierung über Gefahren für die nationale Sicherheit aufzuklären, damit diese entsprechend handeln kann.[1] Der Aufbau und die Struktur der Nachrichtendienste in den aufgezählten Ländern unterscheidet sich jedoch in einigen Aspekten, z.B. der Trennung zwischen dem Auslands- und Inlandsnachrichtendienst sowie der Trennung zu anderen nationalen Sicherheitsbehörden.[2] Dies kann sich auf die einzelnen Zuständigkeitsbereiche und damit auch die einzelnen Befugnisse auswirken. Hinzukommen vor allem die unterschiedlichen Vorgaben der Rechtssysteme, die die Vergleichbarkeit der Befugnisse der Nachrichtendienste erschweren, wie die Wirkung von Gerichtsentscheidungen oder das Vorliegen bzw. der Umfang eines verfassungsrechtlichen Gesetzesvorbehalts. Außerdem ist die gesetzliche Gestaltung des Nachrichtendienstrechtes in allen Ländern permanent in Bewegung, unter anderem wegen Ereignissen, die nachrichtendienstliche Tätigkeiten in Frage stellen, oder Gerichtsentscheidungen, die nachrichtendienstliche Befugnisse für rechtswidrig erklären. Insoweit ist insbesondere bei der Betrachtung und Zusammenfassung des aktuellen Stands der rechtswissenschaftlichen Diskussion zu berücksichtigen, dass sich die Ausführungen möglicherweise auf bereits veraltete Rechtslagen beziehen können.

Bevor nachfolgend ein Überblick über die Diskussion innerhalb der rechtswissenschaftlichen Literatur zu den genannten Nachrichtendiensten erfolgt (dazu unter 2.), werden die Nachrichtendienste der jeweiligen Länder und die jeweiligen Rechtsgrundlagen übersichtsartig in Tabellen zusammengefasst und gegenübergestellt. Wegen der Komplexität der verschiedenen Rechtssysteme und der Dynamik des Nachrichtendienstrechtes in allen vorliegend betrachteten Ländern beschränkt sich die weitere Darstellung auf die aktuelle Struktur und Organisation der einzelnen Nachrichtendienste sowie die einfachgesetzlich geregelten Rechtsgrundlagen, soweit sich hierzu Literatur finden lässt (dazu unter 3.). Abschließend werden exemplarisch die jeweiligen Befugnisse aus den Ländern zur gezielten Telekommunikationsüberwachung und die einfachgesetzlich bestimmten Voraussetzungen näher erörtert, ebenfalls soweit sich hierzu Literatur finden lässt (dazu unter 4.).

---

1 Zum Begriff des Nachrichtendienstes und zur Abgrenzung zu Geheimdiensten, Dietrich, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, III § 3 Rn. 7.

2 Vgl. zum Trennungsgebot, Wissenschaftliche Dienste des Deutschen Bundestages, Zum Trennungsgebot zwischen Polizei und Nachrichtendiensten, WD 3 - 3000 - 071/23, 01.09.2023.

DE	USA	UK	FR	NL	FIN
Bundesamt für Verfassungsschutz (BfV) Landesverfassungsschutzbehörden (LfV) Bundesnachrichtendienst (BND) Militärischer Abschirmdienst (MAD)	u.a.[3] Federal Bureau of Investigation (FBI)[4] Department of Homeland Security (DHS) Central Intelligence Agency (CIA) National Security Agency (NSA) Defense Intelligence Agency (DIA)	Security Service (MI 5) Secret Intelligence Service (MI 6) Gouvernement Communications Headquarters (GCHQ) Defence Intelligence Staff (DIS)	u.a.[5] La direction générale de la sécurité intérieure (DGSI) La direction générale de la sécurité extérieure (DGSE) La direction du reseignement militaire (DRM)	Algemene Inlichtingen- en Veiligheidsdienst (AIVD) Militaire Inlichtingen- en Veiligheidsdienst (MIVD)	Suojelupoliisi (SUPO) Defence Command Intelligence Division of the Finnish Defence Forces

Tabelle 1 (Übersicht zu den Nachrichtendiensten)

DE	USA	UK	FR	NL	FIN
Bundesnachrichtendienstgesetz (BNDG) Bundesverfassungsschutzgesetz (BVerfSchG) Gesetz über den	Title 50 USC Ch. 36: Foreign Intelligence Surveillance (50 USC §§ 1801 ff.) Executive Order 12333 - United States Intelligence	Security Service Act (SS 1989) Intelligence Services Act (ISA 1994) Investigatory Powers Act (IPA 2000)	Code de la sécurité intérieure (CSI) Code de la défense	Wet op de inlichtingen - en veiligheidsdiensten, (Gesetz über den Sicherheits- und Nachrichtendienst) (Wiv 2017)	Poliisilaki (Polizeigesetz) (872/2011) Laki tietoliikennetiedustelusta siviilitiedustelussa (Gesetz zur Telekommunikationsüberwachung

3 In den USA gibt es die Intelligence Community (IC), die 18 verschiedene Nachrichtendienste umfasst, dazu mehr auf: https://www.intelligence.gov/how-the-ic-works.

4 Das FBI ist streng genommen kein Nachrichtendienst, sondern die Bundespolizei, verfügt jedoch über nachrichtendienstliche Befugnisse, dazu mehr auf: https://www.fbi.gov/investigate/how-we-investigate/intelligence.

5 Auch in Frankreich gibt es mehrere Nachrichtendienste, vgl. dazu Art. R811-1 CSI.

DE	USA	UK	FR	NL	FIN
Militärischen Abschirmdienst (MADG) Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Art. 10-Gesetz (G 10)	Activities (E.O. 12333)	Investigatory Powers Act (IPA 2016)			durch die SUPO) (582/2019) Valtioneuvoston asetus siviilitiedustelusta (Regierungsdekret) (709/2019) Laki sotilastiedustelusta (Gesetz über den militärischen Nachrichtendienst) (590/2019)

Tabelle 2 (Rechtsgrundlagen der Nachrichtendienste)

Maßnahme	D	USA	UK
Gezielte Telekommunikationsüberwachung	§§ 3, 1 Abs. 1 Nr. 1 G 10	50 USC § 1802 ff. („Electronic surveillance“) 50 USC § 1881a („[…] targeting certain persons outside the United States other than United States persons”) 50 USC § 1881b („Certain acquisitions inside the United States targeting United States persons outside the United States”) 2.3. E.O. 12333 (vgl. zum Bereich der Strafverfolgung, 18 USC §§ 2510 bis 2522)	v.a. zu „targeted interception warrants“: Sec. 15(a) ff. IPA 2016

Maßnahme	**D**	**USA**	**UK**
Strategische Fernmeldeaufklärung	§§ 5 Abs. 3, 8 Abs. 1 Satz 1, 1 Abs. 1 Nr. 2 G 10 (mit Inlandsbezug) § 19 Abs. 1 BNDG (Ausländer im Ausland)	2.3. E.O. 12333 (vgl. ferner zur "bulk collection" Sec. 2(c)(ii) E.O. 14086)	„Bulk interception warrants": Sec. 136 ff. IPA 2016
Übermittlung an inländische Nachrichtendienste	§§ 6, 19 Abs. 1 Satz 1, 20 Abs. 1 Satz 3 BVerfSchG §§ 4 Abs. 2 Satz 3, 7, 8 G 10 §§ 11 Abs. 1, 29 Abs. 1, 38 Abs. 1 BNDG §§ 3 Abs. 3, 11 Abs. 1 MADG	„Use of information": 50 USC § 1806 50 USC § 1825 50 USC § 1842	„Safeguards relating to retention and disclosure of material"/„Disclosure of retained data": Sec. 53, 93, 129, 150, 171, 191 IPA 2016
Übermittlung an inländische Polizei- und Strafverfolgungsbehörden	§§ 19 Abs. 1, 20 Abs. 1 Satz 1 BVerfSchG §§ 11 Abs. 2, 29 Abs. 3, Abs. 4, 38 Abs. 2, Abs. 4 BNDG § 11 Abs. 2 MADG	„Use of information": 50 USC § 1806 50 USC § 1825 50 USC § 1842	„Safeguards relating to retention and disclosure of material"/„Disclosure of retained data": Sec. 53, 93, 129, 150, 171, 191 IPA 2016
Übermittlung an sonstige inländische Behörden	§ 19 Abs. 1 Satz 2 BVerfSchG § 4 Abs. 4 G 10 § 11 Abs. 2 BNDG § 11 Abs. 1 MADG	„Use of information": 50 USC § 1806 50 USC § 1825 50 USC § 1842	„Safeguards relating to retention and disclosure of material"/„Disclosure of retained data": Sec. 53, 93, 129, 150, 171, 191 IPA 2016
Übermittlung an ausländische Stellen	§ 19 Abs. 3 BVerfSchG § 11 Abs. 1 MADG	„Use of information": 50 USC § 1806 50 USC § 1825 50 USC § 1842	„Safeguards relating to disclosure of material overseas": Sec. 54, 130, 151, 192 IPA 2016

Tabelle 3 (Relevante Rechtsgrundlagen der Befugnisse zur Informationsbeschaffung und -übermittlung in D/USA/UK)

Maßnahme	**F**	**NL**	**FIN**[6]
Gezielte Telekommunikationsüberwachung	L852-1 CSI	Art. 47 Wiv 2017	Kap. 5a Sec. 6 des Polizeigesetzes Sec. 7, 9 des Gesetzes zur Telekommunikationsüberwachung durch die SUPO Sec. 34 des Gesetzes über den militärischen Nachrichtendienst
Strategische Fernmeldeaufklärung	Art. L854-1 bis L854-9 CSI	Art. 48 Wiv 2017	Kap. 5a Sec. 7 des Polizeigesetzes („Decision on traffic data monitoring in civilian intelligence“)
Übermittlung an inländische Nachrichtendienste	L822-3 II CSI	Art. 61 Wiv 2017 Art. 86 Wiv 2017	Kap. 5a Sec. 54, Sec. 56, Sec. 58 des Polizeigesetzes Sec. 10 Sec. 17 des Gesetzes zur Telekommunikationsüberwachung durch die SUPO Sec. 15, Sec. 17, Sec. 19, Sec. 79 des Gesetzes über den militärischen Nachrichtendienst
Übermittlung an inländische Polizei- und Strafverfolgungsbehörden	[/][7]	Art. 66 Wiv 2017	Kap. 5a Sec. 44 des Polizeigesetzes Sec. 17 des Gesetzes zur Telekommunikationsüberwachung durch die SUPO

6 Die Informationen beruhen auf einer Auskunft Finnlands nach Anfrage der Wissenschaftlichen Dienste des Deutschen Bundestages.

7 Weitere französische Vorschriften, die die Informationsübermittlung durch französische Nachrichtendienste an andere Stellen als inländische Nachrichtendienste regeln, ließen sich mit der verfügbaren Literatur nicht finden.

Maßnahme	F	NL	FIN[6]
			Sec. 79 des Gesetzes über den militärischen Nachrichtendienst
Übermittlung an sonstige inländische Behörden	[/][7]	Art. 62 Wiv 2017	Kap. 5a Sec. 55 des Polizeigesetzes Sec. 18 des Gesetzes über den militärischen Nachrichtendienst
Übermittlung an ausländische Stellen	[/][7]	Art. 62 Wiv 2017 Art. 64 Wiv 2017 Art. 88 Wiv 2017	Kap. 5a Sec. 57 des Polizeigesetzes Sec. 20 des Gesetzes über den militärischen Nachrichtendienst

Tabelle 4 (Relevante Rechtsgrundlagen der Befugnisse zur Informationsbeschaffung und -übermittlung in F/NL/FIN)

2. Stand der Diskussion innerhalb der Literatur

Innerhalb der rechtswissenschaftlichen Literatur wird insbesondere das US-amerikanische Nachrichtendienstrecht im Verhältnis zum deutschen Nachrichtendienstrecht analysiert und diskutiert. Dabei stehen diejenigen Befugnisse der US-amerikanischen Nachrichtendienste im Fokus, auf deren Grundlage umfangreiche Daten und Informationen beschafft werden. So wird zum Teil als Besonderheit gegenüber dem deutschen Nachrichtendienstrecht angeführt, dass die staatlichen Ermittlungsmaßnahmen im Rahmen der nachrichtendienstlichen Befugnisse keine bestimmte Eingriffsschwelle oder keinen bestimmten Verdachtsgrad voraussetzen würden.[8] Außerdem sei anders als im deutschen Recht eine anlasslose Massenüberwachung unter bestimmten Voraussetzungen zulässig.[9] Allerdings ist in diesem Zusammenhang die Rechtslage veraltet, weil die in den entsprechenden Ausführungen diskutierte Rechtsgrundlage so nicht mehr besteht (vgl. zu 50 USC § 1861 a.F. näher unter 3.2.1). Dennoch wird vereinzelt – unabhängig von der Rechtsentwicklung in den USA – grundsätzlich im Vergleich auf „strenge Gesetze“ in Deutschland hingewiesen.[10]

Ausgangspunkt der Diskussion ist regelmäßig ein Vergleich des Schutzes personenbezogener Daten in den jeweiligen Ländern. So wird vertreten, dass das Grundgesetz höhere Anforderungen an

8 Lang, Geheimdienstinformationen im deutschen und amerikanischen Strafprozess, 2014, S. 213.

9 Knaust, Matrix einer neuen Generation auslandsnachrichtendienstlicher Überwachungstätigkeit, 2023, S. 80.

10 Linzbach/Vell, Diskussionsbericht Panel 1: Nachrichtendienstrecht im Rechtsvergleich – Grundlinien und jüngere Entwicklungen, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 137 (139).

das deutsche Auslandsnachrichtendienstrecht als z.B. das US-amerikanische Rechtssystem stelle, „wo die Gewährleistungen der Bill of Rights entgegen den universalistischen Ursprüngen überwiegend national verstanden werden“.[11] Es wird kritisiert, dass sich nach dem geltenden US-amerikanischen Recht keiner sicher sein könne, „ob seine Telefongespräche, Emails etc. durch US-Nachrichtendienste erfasst und verarbeitet werden“.[12] Im Jahr 2020 entschied der Europäische Gerichtshof (EuGH) im Zusammenhang mit der Übermittlung von personenbezogenen Daten in die USA und besonders wegen mangelnden Rechtsschutzmöglichkeiten, dass „nicht angenommen werden kann, dass die auf [US-amerikanisches Nachrichtendienstrecht] gestützten Überwachungsprogramme auf das zwingend erforderliche Maß beschränkt sind“.[13] In Reaktion auf diese Entscheidung des EuGH wurden durch die Executive Order 14086 des US-amerikanischen Präsidenten „Enhancing Safeguards for United States Signals Intelligence Activities“ (kurz E.O. 14086)[14] neue US-amerikanische Vorgaben zum Schutz von personenbezogenen Daten auch von Nicht-US-Personen erlassen. Diese seien Stimmen der Literatur zufolge allerdings keine Verbesserung für den Schutz von nationalen und europarechtlichen Grundrechten, sondern erforderlich sei vielmehr eine „umfassende Reform der Massenüberwachung durch US-Geheimdienste […] [, f]ür eine solche […] den USA wiederum der politische Wille [fehle]“.[15]

Demgegenüber werden die Befugnisse von französischen, britischen, niederländischen und finnischen Nachrichtendiensten nur kaum bis gar nicht in der deutschen rechtswissenschaftlichen Literatur diskutiert, oder die Darstellungen beziehen sich auf eine veraltete Rechtslage.[16] Das Bundesverfassungsgericht (BVerfG) stellte allerdings im Jahr 2020 verschiedene Rechtsregime im Vergleich gegenüber: „[…] international [ist es] nicht unüblich, Rechtsgrundlagen für auch auf Ausländer im Ausland bezogene Überwachungsmaßnahmen zu schaffen. Sie haben allein eine innerstaatliche Ermächtigungsfunktion“ und wies auf die Rechtslage in den USA, im Vereinigten Königreich und in Frankreich hin.[17] Der Europäische Gerichtshof für Menschenrechte (EGMR) stellte im Jahr 2021 fest, dass in sieben Vertragsstaaten (dazugehörend auch Finnland, Frankreich, Deutschland, die Niederlande und das Vereinigte Königreich) die ungezielte Überwachung

---

11 Knaust, Matrix einer neuen Generation auslandsnachrichtendienstlicher Überwachungstätigkeit, 2022, S. 593.

12 Wischmeyer, Überwachung ohne Grenzen, 2017, S. 99, auch zu einem Zitat aus einer Präsentation des Office of Gen. Counsel NSA, Slide 83 „There are very few things we cannot accomplish within the existing rules“.

13 EuGH, Urteil vom 16.07.2020 - C-311/18, Rn. 181 ff.

14 Executive Order 14086 „Enhancing Safeguards for United States Signals Intelligence Activities“ vom 07.10.2022 (E.O. 14086), aufgenommen im USC unter 50 USC § 3001; eine E.O. ist eine Verfügung des Präsidenten, mit der er die Tätigkeiten der Exekutive steuert, vgl. dazu https://www.federalregister.gov/presidential-documents/executive-orders.

15 Glocker, EU-US Data Privacy Framework: Update des Privacy Shield mit Augenmaß, ZD 2023, 189 (193 f.).

16 Vgl. am aktuellsten die Darstellung zur Massenüberwachung nach französischen Recht, Knaust, Matrix einer neuen Generation auslandsnachrichtendienstlicher Überwachungstätigkeit, 2022; siehe ferner Warusfel, The new French intelligence law, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 129 ff. Vgl. zum britischen Nachrichtendienstrecht McKay/Walker, Intelligence law in the United Kingdom, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 119 ff. Zur alten Rechtslage in Frankreich, Krumrey, Die Inlandsnachrichtendienste in Frankreich und Deutschland, 2014.

17 BVerfG, Urteil vom 19.05.2020 - 1 BvR 2835/17, Rn. 103.

von kabelgebundenen und -losen Kommunikationen („bulk interception“) offiziell stattfindet.[18] Zum Teil können – neben der Rechtsprechung – wissenschaftliche Beiträge außerhalb des deutschsprachigen Raumes Aufschluss über die aktuelle Rechtslage und die Diskussionen im jeweiligen Land geben.[19]

3. Struktur und Rechtsrahmen des Nachrichtendienstrechts

3.1. Deutschland

In Deutschland existieren auf Bundesebene drei Nachrichtendienste: der Inlandsnachrichtendienst Bundesamt für Verfassungsschutz (BfV),[20] der Auslandsnachrichtendienst Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD). Die Zuständigkeitsbereiche, Aufgaben und Befugnisse sind ausführlich im Bundesverfassungsschutzgesetz (BVerfSchG)[21], im BND-Gesetz (BNDG)[22] und im MAD-Gesetz (MADG)[23] geregelt. Das BNDG und das MADG verweisen häufig auf Regelungen des BVerfSchG. Des Weiteren ist das G 10 Gesetz (G 10)[24] für bestimmte Maßnahmen relevant, die in den Schutzbereich des Brief-, Post- und Fernmeldegeheimnisses nach Art. 10 des Grundgesetzes (GG)[25] eingreifen. Nach § 3 Abs. 1 BVerfSchG ist es die Aufgabe der Bundes- und Landesverfassungsschutzbehörden, Informationen über im Gesetz näher bestimmte Bestrebungen, die unter anderem die nationale Sicherheit gefährden, und sicherheitsgefährdende oder geheimdienstliche Tätigkeiten zu sammeln und auszuwerten. Nach § 1 MADG hat der MAD im Bereich der Bundeswehr ähnliche Aufgaben wie das BfV und gilt als

18 EGMR, Urteil vom 25.05.2021 - 58170/13, 62322/14, 24960/15, Rn. 242.

19 Vgl. zur Rechtslage in Frankreich Tréguer, Overview of France’s Intelligence Legal Framework, Centre de recherches internationales (CERI), publiziert auf HAL open science, 2021; zur Rechtslage in den Niederlanden, dazu Eijkman/Eijk/van Schaik, Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?, 2018; zur Rechtslage in Finnland, Lohse, The Intelligence Process in Finland, Scandinavian Journal of Military Studies, Vol. 3, 2020/1, 68.

20 Auf Landesebene gibt es in Deutschland in jedem Bundesland eigene Landesverfassungsschutzämter (LfV), deren rechtlichen Grundlagen vorliegend nicht näher erörtert werden.

21 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz - BVerfSchG) vom 20.12.1990 (BGBl. I S. 2954, 2970), zuletzt geändert am 19.12.2022 (BGBl. I S. 2632).

22 Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG) vom 20.12.1990 (BGBl. I S. 2954, 2979), zuletzt geändert am 05.07.2021 (BGBl. I S. 2274).

23 Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz - MADG) vom 20.12.1990 (BGBl. I S. 2954), zuletzt geändert am 05.07.2021 (BGBl. I S. 2274).

24 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) vom 26.06.2011 (BGBl. I S. 1254, 2298, 154), zuletzt geändert am 05.07.2021 (BGBl. I S. 2274).

25 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert am 19.12.2022 (BGBl. I S. 2478).

„Verfassungsschutz“ der Bundeswehr.[26] Der BND darf gemäß § 1 Abs. 2 Satz 1 BNDG und § 2 Abs. 1 BNDG Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, verarbeiten.

Zum besseren Verständnis des deutschen Nachrichtendienstrechtes und der jeweiligen Befugnisse ist das sog. Trennungsgebot von Bedeutung. Dieses ist in §§ 2 Abs. 1 Satz 3, 8 Abs. 3 BVerfSchG, § 1 Abs. 1 Satz 2 BNDG und § 4 Abs. 2 MADG ausdrücklich geregelt. Es gebietet eine strikte organisatorische und sachliche Trennung von Polizeibehörden und Nachrichtendiensten.[27] Danach bestehen für Nachrichtendienste ein Exekutivverbot und ein Verbot der Nutzung polizeilicher Befugnisse, vor allem polizeilicher Zwangsbefugnisse, wie Vernehmungen, Durchsuchungen, Beschlagnahmen.[28] Das Trennungsgebot verbietet jedoch nicht jedes Zusammenwirken von Nachrichtendiensten mit Polizei- und Strafverfolgungsbehörden. So ist, wie nachstehend erläutert, die Zusammenarbeit in Form der Übermittlung von Informationen unter bestimmten Voraussetzungen zulässig. In den anderen vorliegend betrachteten Ländern gibt es kein vergleichbares Trennungsgebot.[29] Das deutsche Nachrichtendienstrecht ist darüber hinaus besonders durch die Rechtsprechung des Bundesverfassungsgerichts zum Schutz des allgemeinen Persönlichkeitsrechts in seiner Ausprägung als Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG) geprägt. Dieses hat in den letzten Jahren eine Vielzahl an Entscheidungen getroffen, die sich unmittelbar auf die Geltung nachrichtendienstlicher Vorschriften ausgewirkt haben. Erst zuletzt hat es entschieden, dass bestimmte Übermittlungsvorschriften des BVerfSchG gegen das Recht auf informationelle Selbstbestimmung verstoßen und die entsprechenden Vorschriften für nichtig erklärt (näher dazu unter 3.1.2.).[30]

3.1.1. Informationsbeschaffung

Das deutsche Nachrichtendienstrecht unterscheidet im Wesentlichen zwischen der offenen (§ 8 Abs. 1 BVerfSchG; § 2 BNDG)[31] und der heimlichen Informationsbeschaffung (§ 8 Abs. 2 BVerfSchG; § 5 Satz 1 BNDG; § 4 Abs. 1 Satz 1 MADG). Die Informationsbeschaffung ist offen, wenn die zu beschaffenden Informationen für jedermann zugänglich sind, d.h. sich aus offenen

---

26 Gusy, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, IV § 1 Rn. 81. Außerhalb der bundesdeutschen Grenzen ist der MAD im Rahmen von Auslandsverwendungen der Bundeswehr zuständig, § 14 MADG, vgl. dazu Droste, Handbuch des Verfassungsschutzrechts, 1. Aufl. 2007, Teil 4, S. 654.

27 Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, B. Rn. 257.

28 Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, B. Rn. 257 f.; zum Verbot polizeilicher Zwangsbefugnisse, BVerfG, Nichtannahmebeschluss vom 09.11.2010 - 2 BvR 2101/09, Rn. 59.

29 Vgl. dazu die Übersicht der Wissenschaftlichen Dienste des Deutschen Bundestages, Zum Trennungsgebot zwischen Polizei und Nachrichtendiensten, WD 3 - 3000 - 071/23, 01.09.2023.

30 BVerfG, Beschluss vom 28.09.2022 - 1 BvR 2354/13, Tenor.

31 § 4 Abs. 1 Satz 1 MADG verweist zwar nur auf die heimliche Informationsbeschaffung gemäß § 8 Abs. 2 BVerfSchG, was jedoch innerhalb der rechtswissenschaftlichen Literatur teleologisch ausgelegt wird, dass erst recht weniger eingriffsintensive Maßnahmen der offenen Informationsbeschaffung zulässig sind, dazu Löffelmann, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, VI § 5 Rn. 59.

Quellen ergeben.[32] Die heimliche Informationsbeschaffung umfasst indes Methoden, Gegenstände und Instrumente, „wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen“ (§ 8 Abs. 2 Satz 1 BVerfSchG; § 5 Satz 1 BNDG; § 4 Abs. 1 Satz 1 MADG).[33] Als besondere Formen der Datenerhebung sind im Zusammenhang mit der heimlichen Informationsbeschaffung die akustische und optische Überwachung von Wohnungen (§ 9 Abs. 2 BVerfSchG; § 5 Satz 2 BNDG; § 5 MADG), die Ermittlung von Mobilfunkdaten (§ 9 Abs. 4 BVerfSchG; § 5 Satz 2 BNDG; § 5 MADG), der Einsatz von verdeckten Mitarbeitern (§ 9a BVerfSchG; § 5 Satz 2 BNDG; § 5 MADG) und von Vertrauensleuten (§ 9b BVerfSchG; § 5 Satz 2 BNDG; § 5 MADG) geregelt.

Im G 10 sind die besonderen Befugnisse zur Telekommunikationsüberwachung und zur Öffnung von Sendungen, die die Inlandskommunikation betreffen und dem nach Art. 10 GG verfassungsrechtlich geschützten Brief- oder Postgeheimnis unterliegen, geregelt. So richtet sich die gezielte bzw. auf ein Individuum gerichtete Telekommunikationsüberwachung nach §§ 3, 1 Nr. 1 G 10. Ferner dürfen die Nachrichtendienste gemäß § 11 Abs. 1a G 10 zur Überwachung und Aufzeichnung der laufenden sowie ab dem Zeitpunkt der Anordnung ruhenden Telekommunikation in unverschlüsselter Form in ein von dem Betroffenen genutztes informationstechnisches System eingreifen (sog. Quellen-Telekommunikationsüberwachung).

Des Weiteren können die Nachrichtendienste sowohl bei anderen staatlichen Stellen und Behörden um die Übermittlung der zur Erfüllung ihrer Aufgaben erforderlichen personenbezogenen Daten ersuchen (§ 18 Abs. 3 BVerfSchG; § 10 Abs. 3 Satz 1 BNDG; § 10 Abs. 2 Satz 1 MADG) als auch von bestimmten inländischen privaten Stellen (z.B. von Luftfahrtunternehmen, Betreibern von Computerreservierungssystemen oder Telekommunikationsdienstleistern) Auskunft über im Gesetz näher bestimmte Daten, wie Verkehrsdaten, verlangen (§§ 8a, 8b BVerfSchG; § 3 BNDG; § 4a MADG). § 8d BVerfSchG, § 4 BNDG, § 4b MADG regeln die Auskunftsverlangen bei inländischen Telekommunikation- und Telemediendienstleistern nach Bestandsdaten.[34]

Der BND verfügt schließlich über besondere Befugnisse zur Auslandsaufklärung. So darf ausschließlich er grenzüberschreitende Telekommunikation, bei der sich ein Kommunikationsteilnehmer im Inland und ein anderer im Ausland befindet, überwachen und Sendungen öffnen (strategische Fernmeldeaufklärung; §§ 5 Abs. 1 Satz 3 Nr. 2 bis 8, 8 Abs. 1 Satz 1, 1 Abs. 1 Nr. 2 G 10). Bei der strategischen Ausland-Fernmeldeaufklärung, bei der die Kommunikationsteilnehmer Ausländer sind und sich im Ausland befinden, darf nach § 19 Abs. 1 BNDG ebenfalls nur der BND zur Erfüllung seiner Aufgaben personenbezogene Inhaltsdaten von Ausländern im Ausland

---

32 Vgl. zum Begriff der offenen Informationsbeschaffung, BVerwG, Urteil vom 21.07.2010 - 6 C 22/09, NVwZ 2011, 161 (163 Rn. 15); Droste, Handbuch des Verfassungsschutzrechts, 1. Aufl. 2007, Teil 2, S. 227.

33 Die heimlichen Maßnahmen sind in einer Dienstvorschrift näher geregelt (§ 8 Abs. 2 Satz 4 BVerfSchG), die jedoch nicht öffentlich, sondern „VS-Nur für den Dienstgebrauch“ eingestuft ist, vgl. Bergemann, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, H. Rn. 89; vgl. ferner Wissenschaftliche Dienste des Bundestages, Zum Tarnmitteleinsatz durch Nachrichtendienste, 10.03.2022, WD 3 - 3000 - 024/22, S. 5.

34 Bestandsdaten sind Vertragsdaten, „die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses“ gespeichert worden sind und betreffen nicht die Nutzung der jeweiligen Dienste im Einzelnen, siehe Gärditz, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, VI § 1 Rn. 23; Bergemann, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, H. Rn. 84.

mit technischen Mitteln verarbeiten.[35] Die Verarbeitung von Verkehrsdaten richtet sich nach § 26 Abs. 1 BNDG. § 19 Abs. 6 BNDG regelt die Befugnis des BND, sich mit technischen Mitteln Zugang zu informationstechnischen Systemen eines ausländischen Telekommunikations- oder Telemedienanbieters im Ausland zu verschaffen und dabei personenbezogene Daten zu erheben. Zudem darf gemäß § 34 Abs. 1 BNDG nur der BND zur Erfüllung seiner Aufgaben ohne Wissen des Betroffenen auf der Grundlage zuvor angeordneter individueller Aufklärungsmaßnahmen mit technischen Mitteln in von Ausländern im Ausland genutzte informationstechnische Systeme eingreifen und auf ihnen gespeicherte Daten erheben.

Die einzelnen Ermittlungsbefugnisse unterliegen unterschiedlichen Ermittlungs- bzw. Eingriffsschwellen. Die Information muss jedenfalls in der Regel zur Erfüllung der Aufgaben des jeweiligen Nachrichtendienstes erforderlich sein (vgl. allein § 8 Abs. 1 Satz 1 BVerfSchG). Nach § 4 Abs. 1 Satz 5 BVerfSchG ist ferner Voraussetzung für die Informationssammlung und -auswertung durch die Verfassungsschutzbehörden, dass tatsächliche Anhaltspunkte in Bezug auf die Bestrebungen im Sinne des § 3 Abs. 1 BVerfSchG vorliegen. Bei der Bestandsdatenauskunft wird ähnlich vorausgesetzt, dass dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur Aufklärung der in § 3 Abs. 1 BVerfSchG genannten Bestrebungen erforderlich ist. Der Rechtsprechung zufolge sind tatsächliche Anhaltspunkte konkrete und in einem gewissen Umfang verdichtete „Umstände, die bei vernünftiger Betrachtung auf […] Bestrebungen hindeuten und die deshalb weitere Klärung erforderlich erscheinen lassen“.[36] Demnach soll es ausreichend sein, wenn eine „Gesamtschau aller vorhandenen tatsächlichen Anhaltspunkte“ einen Verdacht begründet, auch wenn die einzelnen Umstände selbst noch nicht ausreichend wären.[37] Vor allem bei heimlichen Maßnahmen wird demgegenüber vorausgesetzt, dass Tatsachen die Annahme rechtfertigen, dass dadurch Erkenntnisse insbesondere zur Aufgabenerfüllung gewonnen werden können (§ 9 Abs. 2 BVerfSchG). Ähnlich setzen besondere Auskunftsverlangen voraus, dass Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 3 Abs. 1 BVerfSchG genannten Schutzgüter vorliegen (§ 8a Abs. 1 BVerfSchG). Die Telekommunikationsüberwachung nach § 3 Abs. 1 G 10 setzt tatsächliche Anhaltspunkte für den Verdacht voraus, dass jemand im Straftatenkatalog näher bestimmte Straftaten plant, begeht oder begangen hat. Indes setzt die strategische Fernmeldeaufklärung nach § 5 Abs. 1 G 10 voraus, dass die Kenntnis über Sachverhalte, zu denen Informationen gesammelt werden sollen, zum rechtzeitigen Erkennen und Begegnen von Gefahren für die nationale Sicherheit notwendig ist. § 8 Abs. 1 G 10 fordert wiederum für die Telekommunikationsüberwachung zum Schutz von Leib und Leben einer Person im Ausland, dass die Maßnahme erforderlich ist, damit eine im Einzelfall bestehende Gefahr rechtzeitig erkannt und ihr begegnet werden kann.

---

35 Löffelmann/Zöller, Nachrichtendienstrecht, 2022, C. Rn. 41; die Befugnis erfasst nur die Erhebung personenbezogener Inhaltsdaten („Inhalte einer Individual-Kommunikation“), BT-Drs. 19/26103, S. 56.

36 VGH München, NJW 1994, 748 (749); vgl. ferner dazu BVerwG, Urteil vom 21.07.2010 - 6 C 22/09, NVwZ 2011, 161 (164 Rn. 30) mit Hinweis auf BVerfGE 100, 313 (395).

37 BVerwG, Urteil vom 21.07.2010 - 6 C 22/09, NVwZ 2011, 161 (164 Rn. 30); vgl. dazu ferner Löffelmann, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, VI § 4 Rn. 42 f.

3.1.2. Informationsübermittlung

Die Befugnis der Nachrichtendienste, von ihnen beschaffte Informationen an andere öffentliche oder private Stellen zu übermitteln, ist ebenfalls sehr ausdifferenziert und umfangreich gestaltet. Die Regelungen unterscheiden sowohl nach dem Übermittlungsempfänger sowie teilweise auch nach der Maßnahme, auf deren Grundlage die Informationen beschafft wurden. Besondere Übermittlungsbefugnisse innerhalb der Nachrichtendienste ergeben sich zum Beispiel aus dem Informationsaustausch zwischen den Verfassungsschutzbehörden nach § 6 BVerfSchG und § 3 Abs. 3 MADG. Das BfV übermittelt außerdem auch Informationen an den BND nach § 20 Abs. 1 Satz 3 BVerfSchG. In Bezug auf Daten, die auf der Grundlage einer Telekommunikationsüberwachung beschafft wurden, ist eine Übermittlung innerhalb der Nachrichtendienste nach Stimmen der Literatur nach § 4 Abs. 2 Satz 3 G 10 zulässig.[38] Für die Übermittlung von personenbezogenen Daten an andere deutsche Nachrichtendienste, die der BND gemäß § 5 Abs. 1 G 10 erhoben hat, gilt § 7 Abs. 2 G 10. Für die Übermittlung an andere Sicherheitsbehörden, die regelmäßig mit eigenen operativen Befugnissen ausgestattet sind, gibt es ebenfalls eine Vielzahl besonderer Regelungen. Nach § 19 Abs. 1 Satz 1 BVerfSchG (§ 11 Abs. 1 Satz 1 MADG; § 11 Abs. 1 Satz 2 BNDG) dürfen die Nachrichtendienste Informationen übermitteln und nach § 20 Abs. 1 Satz 1 BVerfSchG (§ 11 Abs. 2 MADG; § 11 Abs. 3 BNDG) sind sie unter bestimmten Voraussetzungen zur Übermittlung verpflichtet. Die Übermittlung von personenbezogenen Daten an andere inländische öffentliche Stellen richtet sich grundsätzlich nach § 19 Abs. 1 Satz 2 BVerfSchG (§ 11 Abs. 1 Satz 1 MADG; § 11 Abs. 1 Satz 1 BNDG), jene an ausländische öffentliche Stellen nach § 19 Abs. 3 BVerfSchG (§ 11 Abs. 1 Satz 1 MADG; § 11 Abs. 2 BNDG) und jene an sonstige, insbesondere private Stellen, nach § 19 Abs. 4 BVerfSchG (§ 11 Abs. 1 Satz 1 MADG; § 11 Abs. 2 BNDG). Für die Übermittlung von personenbezogenen Daten, die der BND im Rahmen der Ausland-Fernmeldeaufklärung erhoben hat, gelten die besonderen Übermittlungsvorschriften des § 29 BNDG. Die Vorschrift differenziert auch nach dem Zweck, zu dem der BND die Daten erhoben hat. Ähnlich regelt § 38 BNDG die Übermittlung von personenbezogenen Daten aus individuellen Aufklärungsmaßnahmen.

Im Zusammenhang mit den Übermittlungsvorschriften und mit Blick auf die gesetzliche Gestaltung der Übermittlungsschwellen ist die Rechtsprechung und insbesondere der erst kürzlich ergangene Beschluss des Bundesverfassungsgerichts zu beachten, wonach unter anderem § 20 Abs. 1 Satz 1 und Satz 2 BVerfSchG gegen das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verstoßen, soweit sie zur Übermittlung personenbezogener Daten verpflichten, die mit nachrichtendienstlichen Mitteln, d.h. im Sinne von § 8 Abs. 2 BVerfSchG, erhoben wurden.[39] Das Bundesverfassungsgericht führt mit der Entscheidung seine Rechtsprechung zur Erhebung personenbezogener Daten durch öffentliche Stellen sowie zum Austausch

---

38 Siems, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, VI § 7 Rn. 97.

39 BVerfG, Beschluss vom 28.09.2022 - 1 BvR 2354/13, Tenor: Die Regelungen gelten längstens bis zum 31.12.2023 „mit der Maßgabe fort, dass eine Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten nur zum Schutz eines Rechtsguts von herausragendem öffentlichem Interesse zulässig ist; dem entspricht eine Begrenzung auf besonders schwere Straftaten. Außerdem müssen die nach Maßgabe der Gründe an die jeweilige Übermittlungsschwelle zu stellenden Anforderungen erfüllt sein“. Das Bundesministerium des Innern und für Heimat hat daher Gesetze entworfen, die das Nachrichtendienstrecht entsprechend novellieren sollen, vgl. Bundesregierung, Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts, BT-Drs. 20/8626; Bundesregierung, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes, BT-Drs. 20/8627.

zwischen diesen fort.[40] Wegen der Grundrechtseingriffe durch die Verarbeitung personenbezogener Daten in die informationelle Selbstbestimmung sind je nach Art und Weise der Erhebung oder des Austauschs im Einzelfall an die Rechtsgrundlagen unterschiedliche Anforderungen zu stellen. So hat das Gericht zum einen entschieden, dass der Datenaustausch „sich durch […] einander korrespondierenden Eingriffe von Abfrage und Übermittlung [vollzieht], die jeweils einer eigenen Rechtsgrundlage bedürfen“ (sog. Doppeltür-Grundsatz).[41]

Zum anderen hat das Bundesverfassungsgericht im Zusammenhang mit dem Grundsatz der Zweckbindung von Daten das Kriterium der hypothetischen Neuerhebung entwickelt. Demnach kommt es „[f]ür Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen […] darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften […]. Das Kriterium der Datenneuerhebung gilt allerdings nicht schematisch abschließend und schließt die Berücksichtigung weiterer Gesichtspunkte nicht aus.“[42] Maßgeblich ist demnach für die gesetzliche Gestaltung der jeweiligen Übermittlungsschwelle, „ob der empfangenden Behörde zu dem jeweiligen Übermittlungszweck eine eigene Datenerhebung mit vergleichbar schwerwiegenden Mitteln wie der vorangegangenen Überwachung durch die Verfassungsschutzbehörde erlaubt werden dürfte“, also besonders, ob die empfangende Stelle mit operativen Anschlussbefugnissen ausgestattet ist oder nicht.[43]

3.2. Vereinigte Staaten von Amerika (USA)

Nach aktuellem Stand gibt es in den USA insgesamt 18 öffentliche Stellen, die als Bestandteile der Intelligence Community (kurz IC) offiziell zu den US-amerikanischen Nachrichtendiensten gezählt werden.[44] Die wohl bekanntesten von ihnen sind der Auslandsnachrichtendienst Central Intelligence Agency (CIA), der Informationen über andere Staaten und ihre Staatsangehörige auf der Grundlage menschlicher Quellen (wie verdeckte Ermittler oder Vertrauenspersonen, auf Englisch „human intelligence“, kurz: HUMINT)[45] ermittelt und auswertet,[46] der Auslandsnachrichtendienst National Security Agency (NSA),[47] der hauptsächlich technische Quellen zur Informationsgewinnung (auf Englisch „signals intelligence“, kurz: SIGINT) verwendet, die Bundespolizei Federal Bureau of Investigation (FBI), die neben Strafverfolgungsbefugnissen auch über

---

40 Ausführlich dazu Müller/Schwabenbauer, Datenaustausch zwischen Sicherheitsbehörden, GSZ 2023, 1.

41 Zum sog. Doppeltür-Grundsatz, BVerfG, Beschluss vom 24.01.2012 - 1 BvR 1299/05, Rn. 123; BVerfGE 130, 151 (184).

42 BVerfG, Urteil vom 20.04.2016 - 1 BvR 966, 1140/09, Rn. 287; BVerfGE 141, 220 (327 f.).

43 BVerfG, Beschluss vom 28.09.2022 - 1 BvR 2354/13, Rn. 123.

44 50 USC § 3003(4); vgl. zu den einzelnen Behörden die Übersicht auf der Internetseite der IC, https://www.intelligence.gov/how-the-ic-works; vgl. ferner Congressional Research Service, Defense Primer: National and Defense Intelligence, 29.11.2022.

45 Sec. 1.3.(b)(12)(A)(i) und (ii) der E.O. 12333.

46 50 USC §§ 3035, 3036(c) und (d).

47 50 USC § 3602.

nachrichtendienstliche Befugnisse verfügt,[48] das Department of Homeland Security (DHS) und der militärische Nachrichtendienst Defense Intelligence Agency (DIA). Seit 2004 ist Leiter der IC der Direktor der nationalen Nachrichtendienste (Director of National Intelligence, DNI).[49]

Entsprechend der Vielfalt an Nachrichtendiensten ist auch das Nachrichtendienstrecht in den USA sehr heterogen auf der Grundlage verschiedener Rechtsquellen strukturiert und organisiert.[50] Ein Großteil der relevanten einfachgesetzlichen Vorschriften werden im Gesetzbuch der Vereinigten Staaten (Code of Laws of the United States of America oder auch U.S. Code, im Folgenden USC)[51] zusammengefasst und konsolidiert, wie der National Security Act aus dem Jahr 1947[52] in 50 USC §§ 3001 ff. (Chapter 44 - National Security) und für den Bereich der Auslandsaufklärung der Foreign Intelligence Surveillance Act (FISA) aus dem Jahr 1978[53] in 50 USC §§ 1801 ff. (Chapter 36 - Foreign Intelligence Surveillance).[54] Diese und weitere nachrichtendienstrechtlich relevanten Vorschriften wurden bis heute vielfach geändert und angepasst.[55] Anders als Auslandsaufklärung („foreign intelligence“) und Spionageabwehr („counterintelligence“) ist Inlandsaufklärung („domestic intelligence“) nicht ausdrücklich einfachgesetzlich definiert und die Grenzen zur Auslandsaufklärung, wie sie im deutschen Nachrichtendienstrecht geregelt sind, verschwimmen.[56]

Eine weitere Grundlage für Aktivitäten der US-amerikanischen Nachrichtendienste insgesamt ist die E.O. 12333 des Präsidenten aus dem Jahr 1981.[57] Sie bestimmt Grundsätze für die

---

48 Vgl. dazu Sec. 1.7(g) E.O. 12333.

49 50 USC § 3023.

50 Vgl. für eine ausführliche Übersicht zu den wichtigsten und relevantesten nachrichtendienstlichen Vorschriften bis zum Jahr 2020, Office of the Director of National Intelligence Office of General Counsel, Intelligence Community Legal Reference Book, 2020, abrufbar unter: https://www.dni.gov/files/documents/OGC/IC%20Legal%20Reference%20Book%202020.pdf.

51 Code of Laws of the United States of America vom 30.06.1926 (Pub. L. 69-440, 44 Stat. 777), zuletzt geändert am 06.10.2023 (Pub. L. 118-19, 137 Stat. 106 and 107).

52 National Security Act vom 26.07.1947 (Pub. L. 235; 61 Stat. 496).

53 Foreign Intelligence Surveillance Act (FISA) vom 25.10.1978 (Pub. L. 95-511, 92 Stat. 1783)..

54 „Foreign intelligence information“ definiert gemäß 50 USC § 1801(e); 50 USC 3003(2); vgl. dazu Wischmeyer, Überwachung ohne Grenzen, 2017, S. 24.

55 Z.B. durch Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) vom 26.10.2001 (Pub. L. 107-56, 115 Stat. 272) Intelligence Reform and Terrorism Prevention Act (IRTPA) vom 17.12.2004 (Pub. L. 108-458), Foreign Intelligence Surveillance Act of 1978 Amendments Act (FAA) vom 10.07.2008 (Pub. L. 110-261, 122 Stat. 2473), Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (USA Freedom Act) vom 02.07.2015 (Pub. L. 114-23) und FISA Amendments Reauthorization Act vom 19.01.2018 (Pub. L. 115-118).

56 Siehe ausführlich dazu Congressional Research Service, Intelligence Coordination on Domestic Terrorism and Violent Extremism: Background and Issues for Congress, 01.09.2022, S. 13 ff. m.w.N., S. 17.

57 Executive Order 12333 (United States Intelligence Activities) vom 04.12.1981, zuletzt geändert durch E.O. 13470 vom 30.07.2008.

Informationsermittlung, -aufbewahrung und -übermittlung (Sec. 2.3 E.O. 12333). Nach 1.1. der E.O. 12333 sollen die US-amerikanischen Nachrichtendienste insbesondere dem Präsidenten die erforderlichen Informationen zur Verfügung stellen, mit denen er Entscheidungen im Bereich der Außen-, Verteidigungs- und Wirtschaftspolitik sowie zum Schutz der nationalen Interessen der Vereinigten Staaten vor ausländischen Sicherheitsbedrohungen treffen kann. Wie bereits unter 2. ausgeführt, gibt es seit dem 7. Oktober 2022 die E.O. 14086, die insoweit den Schutz personenbezogener Daten auch für Nicht-US-Personen regelt. Darüber hinaus werden das Nachrichtendienstrecht und die entsprechenden Befugnisse der Nachrichtendienste durch weitere E.O., Richt- und Leitlinien der Verwaltung, Verfügungen und Vorgaben des Präsidenten geregelt, die zum Teil öffentlich zugänglich sind, aber auch zum Teil als Verschlusssachen nicht für die Öffentlichkeit einsehbar sind.[58]

3.2.1. Informationsbeschaffung

Als zentrale Rechtsgrundlage für Informationsbeschaffung im Rahmen der Auslandsaufklärung regelt FISA die elektronische Überwachung („Electronic surveillance“, 50 USC § 1802), physische Durchsuchungen („Physical searches“, 50 USC § 1822), den Einsatz von Geräten zur Abfrage von Informationen über Verbindungsdaten („Pen registers and trap and trace devices“, 50 USC § 1842) und besondere Auskunftsersuchen bei bestimmten privaten Unternehmen zu Geschäftsunterlagen („Access to certain business records for foreign intelligence and international terrorism investigations“ bei „common carrier, public accommodation facility, physical storage facility, or vehicle rental facility“, 50 USC § 1862).

Der bis zum 15. März 2020 geltende 50 USC § 1861 a.F. regelte die Möglichkeit, umfassend Verbindungsdaten zu sammeln („bulk collection“).[59] Die Vorschrift wurde allerdings durch das US-amerikanische Parlament nicht verlängert, sodass die erläuterte Rechtslage mit den besonderen Auskunftsverlangen aus der Zeit vor 2001 ohne die Befugnis, massenhaft Daten zu sammeln, wieder gilt.[60] Dies bedeutet letztlich auch, dass jedenfalls auf der Grundlage des FISA keine umfassenden Datensammlungen mehr zulässig sind. [61] Daten können allerdings noch außerhalb des Anwendungsbereichs des FISA umfassend gesammelt werden, was vor allem Nicht-US-Personen betreffen kann und in den Anwendungsbereich der E.O. 12333 fällt.[62] Informationen über US-

---

58 Vgl. für Maßnahmen durch das FBI die FBI Domestic Investigations and Operations Guide (DIOG) 2021 Version Part 2 of 3; vgl. ferner Morningstar, Distinguishing Between Operational and Intelligence Activities – A Legal Framework, Army Lawyer 2022, Issue 4, 63 (65 f.); Lang, Geheimdienstinformationen im deutschen und amerikanischen Strafprozess, 2014, S. 212: „Neben den ausdrücklich festgelegten Ermächtigungen existiert ein weites Feld sonstiger Ermittlungsmethoden, welche entweder keiner Regulierung zugeführt wurden, der Geheimhaltung unterliegen oder im Ermessen des Präsidenten stehen. Der Einsatz sonstiger Erhebungsmethoden ist damit durchaus denkbar“.

59 Vgl. zur alten Rechtslage, Wischmeyer, Überwachung ohne Grenzen, 2017, S. 27.

60 Ausführlich dazu Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse, 15.11.2021, S. 11.

61 Vgl. übersichtlich zu den Regelungen, Office of the Director of National Intelligence, Annual Statistical Transparency Report, 2023, S. 11, 14, 35

62 Congressional Research Service, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, 17.03.2023, S. 7 f.

Personen sind demgegenüber besonders geschützt. Zum Beispiel sollen die Nachrichtendienste für die Informationssammlung auf der Grundlage von 2.3 und 2.4 E.O. 12333 besondere Verfahren einrichten.[63] Denn nach der herrschenden Ansicht können sich gegen Maßnahmen von US-amerikanischen Nachrichtendiensten nur US-Personen auf den Schutzbereich des 4. Verfassungszusatzes berufen, an den die Dienste jedenfalls im Rahmen der Inlandsaufklärung gebunden sind.[64] Außerdem unterscheidet das US-amerikanische Nachrichtendienstrecht nicht im gleichen Umfang wie im deutschen Nachrichtendienstrecht zwischen personenbezogenen und sonstigen Daten. In diesem Zusammenhang legt allerdings die E.O. 14086 (siehe dazu 50 USC § 3001) neue Anforderungen für die Verarbeitung von personenbezogenen Daten auch zum Schutz von Nicht-US-Personen neu fest. Danach ist außerdem die gezielte Überwachung gegenüber massenhaften Datensammlungen vorrangig; die Maßnahme muss zur Informationsbeschaffung erforderlich („necessary“) sein sowie das Beschaffungsverfahren so gestaltet sein, dass die Beschaffung irrelevanter Information vermieden wird („minimizing the collection of non-pertinent information“).

In Bezug auf Maßnahmen zur elektronischen Überwachung besteht im Übrigen ein Konkurrenzverhältnis zum Electronic Communications Privacy Act (ECPA)[65], der im 18. Kapitel des USC zum Straf- und Strafprozessrecht in den §§ 2510 ff. aufgenommen wurde und in diesem Zusammenhang die Überwachung und Offenlegung von elektronischer Kommunikation regelt. Nach 18 USC § 2511 ist dies verboten, wenn es nicht ausdrücklich erlaubt ist, wie in Bezug auf die elektronische Überwachung nach 50 USC § 1802 (18 USC § 2511(2)(e)).[66]

Neben den einfachgesetzlich geregelten Befugnissen können US-amerikanische Nachrichtendienste, vor allem das FBI, gezielte Auskunftsverlangen auch auf sog. National Security Letters (NSL, schriftliche Anordnungen) stützen, beispielsweise gemäß 18 USC § 2709, 12 USC § 3414, 15 USC § 1681v oder gemäß 15 USC § 1681u.[67]

---

63 Siehe dazu Attorney General Approved U.S. Person Procedures under E.O. 12333, Stand: März 2021, mit weiteren Verlinkungen zu den Richtlinien im Einzelnen.

64 Fourth Amendment, Constitution of the United States: „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized“; vgl. dazu Wischmeyer, Überwachung ohne Grenzen, 2017, S. 24 m.w.N.; siehe ausführlich zu der Bedeutung des 4. Verfassungszusatzes im Zusammenhang mit Maßnahmen zur nationalen Sicherheit, Congressional Research Service, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, 17.03.2023, S. 5 f.; vgl. zur Anwendbarkeit bei Auslandsbezug, Bericht des NSA-Untersuchungsausschusses, BT-Drs. 18/12850, 23.06.2017, S. 243 f.

65 Electronic Communications Privacy Act (ECPA) vom 21.10.1986 (Pub. L. 99-508, 100 Stat. 1848).

66 Vgl. Congressional Research Service, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, 17.03.2023, S. 6.

67 Siehe dazu Office of the Director of National Intelligence, Annual Statistical Transparency Report, 2023, S. 39; vgl. ferner Congressional Research Service, National Security Letters in Foreign Intelligence Investigations: Legal Background, 30.07.2015.

3.2.2. Informationsübermittlung

Für die Übermittlung von einem Nachrichtendienst bereits erhobener Informationen an einen anderen Nachrichtendienst wird durch Sec. 2.3 E.O. 12333 grundsätzlich festgelegt, dass dies zur Prüfung, ob die jeweiligen Informationen für die Tätigkeiten des anderen Nachrichtendienstes relevant und nützlich sind, zulässig ist. Die Übermittlung von Informationen, die durch Methoden der Fernmeldeaufklärung erhoben wurden, ist allerdings nur unter Beachtung besonderer Verfahrensvorschriften (Raw SIGINT Availability Procedures)[68] zulässig. Die Übermittlung von Informationen, die durch Maßnahmen auf der Grundlage des FISA ermittelt wurden, unter anderem an Strafverfolgungsbehörden ist des Weiteren in 50 USC §§ 1806, 1825, 1845 näher einfachgesetzlich geregelt.

Insoweit wird, wie bei der Informationsbeschaffung, grundsätzlich auch die Übermittlung von Informationen über US-Personen speziell geregelt. Sec. 2(c)(iii)(A)(1)(a) der E.O. 14086 sieht allerdings mittlerweile für die Übermittlung von personenbezogenen Informationen auch von Nicht-US-Personen eine besondere Regelung vor, die mit Methoden der Fernmeldeaufklärung erhoben wurden. Danach müssen diese Informationen genauso wie Informationen von US-Personen nach 2.3. der E.O. 12333 behandelt werden.

3.3. Vereinigtes Königreich (UK)

Im UK gibt es den Inlandsnachrichtendienst Security Service, der als MI 5 bekannt ist, den Auslandsnachrichtendienst Secret Intelligence Service, der als MI 6 bekannt ist, den Nachrichtendienst Government Communications Headquarters (GCHQ), der im Wesentlichen für Fernmeldeaufklärung zuständig ist, sowie zuletzt den militärischen Nachrichtendienst Defence Intelligence Staff (DIS).[69]

Das einfachgesetzlich geregelte Nachrichtendienstrecht ergibt sich im Wesentlichen aus dem Security Service Act aus dem Jahr 1989 (SSA 1989)[70], dem Intelligence Service Act (ISA 1994)[71], dem Investigatory Powers Act (IPA 2000)[72], der Maßnahmen wie verdeckte Ermittlungen regelt, und den Investigatory Act 2016 (IPA 2016)[73], der technische Überwachungsmaßnahmen regelt. Daneben sieht Part 4 des Data Protection Act 2018 (DCA 2018)[74] besondere Regelungen für die Datenverarbeitung durch Nachrichtendienste vor.

---

68 Procedures for the Availability or Dissemination of Raw Signal Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333.

69 Vgl. dazu Unterreitmeier, Informationen der Nachrichtendienste: „…Schweigen ist Gold“?, GSZ 2023, 81 (84).

70 Security Service Act 1989 (SSA 1989) vom 27.04.1989 (1989 c. 5).

71 Intelligence Service Act (ISA 1994) vom 26.05.1994 (1994 c. 13).

72 Investigatory Powers Act (IPA 2000) vom 28.07.2000 (2000 c. 23).

73 Investigatory Act 2016 (IPA 2016) vom 29.11.2016 (2016 c. 25).

74 Data Protection Act 2018 (DCA 2018) vom 23.05.2023 (2018 c. 12).

Der gesetzliche Auftrag des Security Service ist nach Sec. 1(2) SSA 1989 vor allem der Schutz der nationalen Sicherheit und insbesondere der Schutz gegen Gefahren durch Spionage, Terrorismus und Sabotage, durch Tätigkeiten von Agenten anderer Staaten und durch Handlungen, die darauf gerichtet sind, die parlamentarische Demokratie mit politischen, wirtschaftlichen oder gewaltsamen Mitteln zu stürzen oder zu untergraben („[…] protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means."). Der gesetzliche Auftrag des Secret Intelligence Service ergibt sich aus Sec. 1 ISA 1994, wonach dieser vor allem Informationen in Bezug auf Handlungen und Bestrebungen von Personen außerhalb der britischen Inseln beschaffen und zur Verfügung stellen soll, wobei die Ausübung der Befugnisse darauf beschränkt sein soll, dass sie nur im Interesse der nationalen Sicherheit mit besonderem Bezug zur Verteidigungs- und Außenpolitik der britischen Regierung, im Interesse des wirtschaftlichen Wohlstands oder in Unterstützung der Verhütung oder Aufdeckung schwerwiegender Straftaten erfolgen.

3.3.1. Informationsbeschaffung

Nicht alle Tätigkeiten und Ermittlungstechniken der Nachrichtendienste sind gesetzlich geregelt, sondern im Wesentlichen nur die, bei denen zu erwarten ist, dass sie in Individualrechte eingreifen können.[75] Innerhalb der Literatur wurden insoweit drei verschiedene Kategorien nachrichtendienstlicher Tätigkeiten unterschieden: 1. Kommunikationsüberwachung, 2. technische und konventionelle Überwachung und 3. Überwachung durch Menschen.[76] Insbesondere die elektronische Überwachung wurde durch IPA 2016 reformiert, einschließlich der Kommunikationsüberwachung (Part 2 IPA 2016), der Beschaffung und Aufbewahrung von Kommunikationsdaten (Part 3, Part 4 IPA 2016), der Eingriffe in Geräte (Part 4 IPA 2016), der Maßnahmen der Massenüberwachung (Part 6 IPA 2016) und der Speicherung umfangreicher personenbezogener Datensätze (Part 7 IPA 2016).

3.3.2. Informationsübermittlung

Die Offenlegung von Informationen, die von den Nachrichtendiensten ermittelt wurden, richten sich nach der jeweiligen Ermittlungsmaßnahme und sind entsprechend danach ausdifferenziert: Die Übermittlung von Informationen, die mit Maßnahmen der Kommunikationsüberwachung ermittelt wurden, richtet sich nach Sec. 53 IPA 2016. Jene, die aufgrund einer Datenbeschaffungsmaßnahme aufbewahrt werden, richtet sich nach Sec. 93 IPA 2016. Jene, die durch Eingriffe in technische Geräte ermittelt wurden, richtet sich nach Sec. 129 IPA 2016. Und entsprechende Maßnahmen in Bezug auf massenhafte Erhebungen („bulk warrants") richten sich nach Sec. 150 IPA 2016, Sec. 171 IPA, 2016 und Sec. 191 IPA 2016. Alle Offenlegungsvorschriften berücksichtigen die Besonderheiten der jeweiligen Ermittlungsmethode, beziehen sich dennoch auf die gleiche Regelungssystematik. So ist darauf zu achten, dass die Offenlegung auf das erforderliche Minimum beschränkt ist, unter anderem in Bezug auf die Anzahl der Personen, denen die Informationen offengelegt werden sollen, als auch das Ausmaß der Offenlegung selbst (vgl. dazu jeweils

75 McKay/Walker, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, IX § 2 Rn. 25.

76 McKay/Walker, Intelligence law in the United Kingdom, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 123.

Abs. 2 der zuvor zitierten Vorschriften).[77] Dies richtet sich nach den Zwecken der genehmigten Offenlegung, die je nach Maßnahme im Gesetz näher definiert werden (vgl. dazu jeweils Abs. 3 der zuvor zitierten Vorschriften). Auch in Bezug auf die Aufbewahrung und Vernichtung der entsprechenden Kopien sollen insoweit besondere Vorkehrungen getroffen werden (vgl. dazu jeweils Abs. 4, Abs. 5 und Abs. 6 der zuvor zitierten Vorschriften). Im Zusammenhang mit vertraulichem journalistischem Material oder der Identifizierung einer journalistischen Quelle bei Informationen ergeben sich außerdem besondere Berichtspflichten an einen „Investigatory Powers Commissioner“ im Fall der Kommunikationsüberwachung und bei Eingriffen in technische Geräte (vgl. Sec. 53(7) IPA 2016 und Sec. 129(8) IPA 2016).

Bezüglich der Übermittlung an Strafverfolgungsbehörden ist zudem Sec. 56 IPA 2016, der den Ausschluss der Verwendung von bestimmten durch Überwachungsmaßnahmen erlangten Informationen in Gerichtsverfahren regelt, zu berücksichtigen. Schedule 3 des IPA 2016 bestimmt allerdings wiederum Ausnahmen dazu.[78]

Die Übermittlung von personenbezogenen Daten an ein Land außerhalb des UK oder an eine internationale Organisation ist einfachgesetzlich geregelt und richtet sich insbesondere nach Sec. 109 DPA 2018. Danach ist eine Übermittlung nach Sec. 109 Abs. 2 DPA 2018 nur zulässig, wenn die Übermittlung eine erforderliche und verhältnismäßige Maßnahme zur Aufgabenerfüllung des zuständigen Nachrichtendienstes ist oder für andere Zwecke nach Sec. 2(2)(a) SSA 1989 oder Sec. 2(2)(a) oder (4)(a) ISA 1994 in Bezug auf den zuständigen Nachrichtendienst. Insoweit sehen insbesondere Sec. 54, 151, 130, 192 IPA 2016 weitere, spezielle Vorkehrungen für die Offenlegung von Informationen außerhalb des UK („overseas“) vor.

3.4. Frankreich

In Frankreich gibt es ebenfalls mehrere Nachrichtendienste („services spécialisés de renseignement“, Art. R811-1 CSI[79]).[80] Dazu gehören vor allem der Auslandsnachrichtendienst Direction générale de la sécurité extérieure (DGSE) und der Inlandsnachrichtendienst Direction générale de la sécurité intérieure (DGSI). Die DGSI ist eine spezielle Kriminalpolizeibehörde („police judiciaire“) im Sinne des Art. 13, 14 des französischen Strafprozessbuches (Code de procédure

77 Vgl. dazu Unterreitmeier, Informationen der Nachrichtendienste: „… Schweigen ist Gold“?, GZS 2023, 81 (84).

78 Weitere Einzelheiten sind insoweit im 11. Teil des Interception of communications code of practice 2022, veröffentlicht am 22.12.2022, geregelt.

79 Code de la sécurité intérieure (CSI) geschaffen durch Ordonnance n°2012-351 vom 12.03.2012.

80 Vgl. übersichtlich bei Warusfel, The new French intelligence law, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 131; ferner Wissenschaftliche Dienste des Bundestages, Nachrichtendienste und ihre Aufgaben in ausgewählten EU-Staaten, WD 3 - 3000 - 382/18, S. 4.

pénale)[81].[82] Zudem gibt es einen militärischen Nachrichtendienst, die Direction du renseignement militaire (DRM).

Bis 2015 beruhten die Tätigkeiten der französischen Nachrichtendienste im Wesentlichen allein auf den Vorschriften, die die einzelnen Nachrichtendienste lediglich eingerichtet haben.[83] Mit Gesetz vom 24. Juli 2015[84] und Gesetz vom 30. November 2015[85] wurde das französische Nachrichtendienstrecht erstmalig umfangreich und einfachgesetzlich konsolidiert und konstituiert.[86] Dazu wurde im Gesetz über die innere Sicherheit (Code de la sécurité intérieure, CSI)[87] ein Achtes Buch zum Nachrichtendienstrecht aufgenommen, das die Ermittlungs- und Übermittlungsbefugnisse ausführlich regelt. Die Aufgabe der Nachrichtendienste wird nach Art. L811-2 CSI näher definiert, wonach diese in Frankreich und im Ausland Informationen besonders über Gefahren für die nationale Sicherheit sammeln und auswerten, um die Regierung aufzuklären und bevorstehende Bedrohungen verhindern zu können. Die Regelungen wurden insbesondere durch Art. 37 des Gesetzes zur Militärplanung für die Jahre 2019 bis 2025 vom 13. Juli 2018[88] und zuletzt durch das Gesetz zur Vermeidung von terroristischen Handlungen und zum Nachrichtendienstrecht vom 30. Juli 2021[89] angepasst und geändert.

3.4.1. Informationsbeschaffung

Die verschiedenen gesetzlichen Voraussetzungen für Ermittlungs- und Informationsbeschaffungsmaßnahmen der Nachrichtendienste ergeben sich vor allem aus Art. L851-1 ff. CSI:[90] insbesondere die Sammlung von „Metadaten“ nach Art. L851-1, L 851-2 CSI, die elektronische Netzwerküberwachung zum Zweck der Terrorismusbekämpfung nach Art. L851-3 CSI, die Echtzeitübermittlung von „Metadaten“ nach Art. L851-4 CSI, die Fernortung bzw. das IMSI-Catching nach

---

81 Code de procédure pénale vom 02.03.1959.

82 Vgl. dazu die Ausführungen auf Französisch: https://www.academie-renseignement.gouv.fr/dgsi.html.

83 Warusfel, The new French intelligence law, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 129.

84 LOI n° 2015-912 relative au renseignement vom 24.07.2015.

85 LOI n° 2015-1556 relative aux mesures de surveillance des communications électroniques internationales vom 30.11.2015.

86 Warusfel, The new French intelligence law, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 129.

87 Code de la sécurité intérieure (CSI) vom 12.03.2012.

88 LOI n° 2018-607 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense vom 13.07.2018.

89 LOI n° 2021-998 relative à la prévention d'actes de terrorisme et au renseignement (1) vom 30.07.2021.

90 Zu einer Übersicht der nachrichtendienstlichen Befugnisse, Tréguer, Overview of France's Intelligence Legal Framework, Centre de recherches internationales (CERI), publiziert auf HAL open science, 2021, S. 5 ff.; Warusfel, The new French intelligence law, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 132.

Art. L851-6 CSI, die Überwachung elektronischer Kommunikation nach Art. L852-1 CSI, die Überwachung offener WLAN-Netzwerke nach Art. L852-2 CSI, die Bild- und Tonaufzeichnung durch das Anbringen von technischen Aufzeichnungsgeräten nach L853-1, gegebenenfalls durch Betreten von Wohnungen und Fahrzeugen nach Art. L853-3 CSI, der Echtzeitzugriff auf Computersysteme nach Art. L853-2 CSI, die Ausland-Fernmeldeaufklärung nach Art. L854-1 CSI, die Nutzung einer falschen Identität nach Art. 861-2 CSI und die Nutzung von Informationen anderer Nachrichtendienste nach Art. 863-1 CSI.[91] Jede dieser Maßnahmen unterliegt der vom CSI vorgesehenen dreigliedrigen Kontrolle durch den Präsidenten, die nationale Kommission zur Kontrolle von nachrichtendienstlichen Maßnahmen (Commission nationale de contrôle des techniques de renseignement, CNCTR) und das höchste französische Verwaltungsgericht (Conseil d'Etat, Art. L841-1 CSI).[92]

Für alle Maßnahmen der Informationsbeschaffung gilt, dass dies nach Art. L801-1 CSI nur im Rahmen der geltenden Gesetze und unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes erfolgen darf.

3.4.2. Informationsübermittlung

Innerhalb der Nachrichtendienste dürfen Informationen nach Art. L822-3 II CSI jedenfalls zur Aufgabenerfüllung im Sinne des Art. Art. L811-3 CSI weitergegeben werden, außer, wenn die Weitergabe der Informationen einen anderen Zweck verfolgt als den, der die Sammlung gerechtfertigt hat (Nr. 1), oder, wenn die zu übermittelnden Informationen mit Methoden erhoben wurden, die die empfangende Stelle nicht anwenden durfte (Nr. 2). Dann setzt die Übermittlung eine Genehmigung des Premierministers nach Art. L821-1 ff. CSI voraus.[93]

3.5. Niederlande

In den Niederlanden gibt es nur zwei Nachrichtendienste: den allgemeinen Nachrichten- und Sicherheitsdienst („Algemene Inlichtingen- en Veiligheidsdienst“, AIVD), der sowohl für die Inlands- als auch für die Auslandsaufklärung zuständig ist, sowie den militärischen Nachrichten- und Sicherheitsdienst („Militaire Inlichtingen- en Veiligheidsdienst“, MIVD), der für die Sicherheit der Streitkräfte zuständig ist und Informationen im Kontext militärischer Tätigkeiten verarbeitet.[94] Das Sicherheits- und Nachrichtendienstgesetz („Wet op de inlichtingen- en veiligheidsdiensten“, Wiv 2017)[95] regelt die einzelnen Zuständigkeiten, Aufgaben und Befugnisse der niederländischen Nachrichtendienste. Insoweit ist zu beachten, dass das Wiv 2017 – anders als vor

---

91 Vgl. ebenfalls zu einer Übersicht der Ermittlungsbefugnisse, Tréguer, Overview of France’s Intelligence Legal Framework, Centre de recherches internationales (CERI), publiziert auf HAL open science, 2021, S. 5 ff.

92 Warusfel, The new French intelligence law, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 132 ff.

93 Vgl. dazu, Tréguer, Overview of France’s Intelligence Legal Framework, Centre de recherches internationales (CERI), publiziert auf HAL open science, 2021, S. 13.

94 Vgl. dazu Eijkman/Eijk/van Schaik, Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?, 2018, S. 15.

95 Wet op de inlichtingen- en veiligheidsdiensten 2017 vom 17.08.2017 (Staatsblad 2017, 317).

allem die deutschen und US-amerikanischen Nachrichtendienstgesetze – weder zwischen nationaler und ausländischer Kommunikation noch zwischen Verkehrs- und Inhaltsdaten unterscheidet.[96]

3.5.1. Informationsbeschaffung

Die Ermittlungsbefugnisse auf der Grundlage des Wiv 2017 können in zwei Kategorien eingeteilt werden: reguläre Befugnisse wie die offene Informationsbeschaffung (Art. 25 Wiv 2017) oder Auskunftsersuchen- und verlangen (Art. 25 und Art. 39 Wiv 2017) und Sonderbefugnisse, die aufgrund der Eingriffsintensität nur in bestimmten Konstellationen wahrgenommen werden dürfen (Art. 8, 10, 28, 40 ff. Wiv 2017).[97] Die Sonderbefugnisse umfassen unter anderem Observationen (Art. 40 Wiv 2017), den Einsatz von verdeckten Ermittlern (Art. 41 Wiv 2017) und die Überwachung von Telekommunikation (Art. 46 ff. Wiv 2017).

3.5.2. Informationsübermittlung

Die Bereitstellung von Informationen innerhalb der Nachrichtendienste richtet sich nach Art. 61 Wiv 2017 und die Bereitstellung an Stellen außerhalb der Nachrichtendienste nach Art. 62 ff. Wiv 2017, wobei besondere Schutzmaßnahmen für die Übermittlung von personenbezogenen Daten nach Art. 68 ff. Wiv 2017 vorgesehen sind. Bei dem Informationsaustausch mit anderen Staaten sehen Art. 88 ff. Wiv 2017 „Prüfvermerke“ vor, die stets aktualisiert werden müssen und Informationen zu den fünf Kriterien liefern sollen, wie im jeweiligen Land die Nachrichtendienste demokratisch eingebettet sind, ob und wie Menschenrechte geachtet werden, welchen Grad an Professionalität die Nachrichtendienste aufweisen, über welche Befugnisse die jeweiligen Nachrichtendienste verfügen und in welchem Ausmaß der Datenschutz gewährleistet ist.[98]

3.6. Finnland

In Finnland gibt es einen zivilen Nachrichtendienst, den Suojelupoliisi (SUPO), und einen militärischen Nachrichtendienst (Defence Command Intelligence Division of the Finnish Defence Forces). Die SUPO ist Teil der Polizei, sodass die Zuständigkeiten, Aufgaben und Befugnisse der zivilen Nachrichtendienste im Kapitel 5a des finnischen Polizeigesetzes[99] (eingefügt durch Gesetzesänderung 581/2019)[100] geregelt sind. Die Befugnisse des militärischen Nachrichtendienstes sind in einem entsprechenden eigenständigen Gesetz geregelt.[101] Weitere relevante Vorschriften

---

96 Siehe dazu Wetzeling/Vieth, Massenüberwachung bändigen, 2019, S. 28, 65.

97 Vgl. dazu Eijkman/Eijk/van Schaik, Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?, 2018, S. 16.

98 Eijkman/Eijk/van Schaik, Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?, 2018, S. 31.

99 Poliisilaki (22.7.2011/872) vom 22.07.2011, in Kraft getreten am 01.01.2014.

100 Laki poliisilain muuttamisesta vom 26.04.2019 (581/2019) vom 26.04.2019, in Kraft getreten am 01.06.2019.

101 Laki sotilastiedustelusta (26.4.2019/590) vom 26.04.2019, in Kraft getreten am 01.06.2019, inoffizielle englische Übersetzung abrufbar unter: https://www.finlex.fi/fi/laki/kaannokset/2019/en20190590.pdf.

für die nachrichtendienstlichen Tätigkeiten ergeben sich insoweit aus dem Gesetz zur Telekommunikationsüberwachung durch die SUPO[102] und dem Regierungsdekret über die SUPO[103]. Diese Gesetze setzten eine Änderung der finnischen Verfassung voraus. Weitere für das finnische Nachrichtendienstrecht relevante Gesetze sind unter anderem das Gesetz über die Kontrolle nachrichtendienstlicher Aktivitäten,[104] das Gesetz über die Verarbeitung von personenbezogenen Daten durch die Polizei[105] und das Gesetz über Zwangsmaßnahmen.[106]

Nach Kapitel 5a Sec. 1 des Polizeigesetzes ist es Aufgabe der SUPO, Informationen zum Schutz der nationalen Sicherheit, zur Unterstützung bei der Entscheidungsfindung der obersten Staatsführung und für die Wahrnehmung gesetzlicher Aufgaben durch andere Behörden im Zusammenhang mit der nationalen Sicherheit zu beschaffen und zu verwenden.[107] Kapitel 5a Sec. 3 des Polizeigesetzes bestimmt des Weiteren die Ziele der SUPO.[108] Die Methoden der Informationsbeschaffung durch die SUPO sind in Kapitel 5a Sec. 2 des Polizeigesetzes aufgezählt, wie unter anderem die Telekommunikationsüberwachung, verdeckte Informationsbeschaffung, technische Überwachung von Geräten oder auch verdeckte Ermittlungen. Die Methoden der Informationsbeschaffung des militärischen Nachrichtendienstes sind entsprechend im 4. Kapitel des Gesetzes zum militärischen Nachrichtendienst geregelt und umfassen ebenfalls unter anderem Maßnahmen wie Telekommunikationsüberwachung, Observationen oder die technische Überwachung von Geräten. Informationen über die Anwendung der Methoden durch die finnischen Nachrichtendienste sind gemäß Sec. 24 des Gesetzes über die Öffentlichkeit der Aktivitäten der Regierung (Act on the Openness of Government Activities)[109] vertraulich und daher nicht zugänglich.

Die Übermittlung von Informationen, die finnische Nachrichtendienste ermittelt oder erlangt haben, ist ebenfalls in den erläuterten Gesetzen speziell geregelt. So können Informationen innerhalb der Nachrichtendienste im Sinne einer Kooperation weitergegeben werden (z.B. Kapitel 5a Sec. 54 des Polizeigesetzes, Sec. 10 des Gesetzes zur Telekommunikationsüberwachung durch die SUPO und Sec. 17 des Gesetzes zum militärischen Nachrichtendienst). Die Übermittlung an Strafverfolgungsbehörden ist z.B. unter den Voraussetzungen nach Kapitel 5a Sec. 44 des

---

102 Laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019) vom 26.04.2019, in Kraft getreten am 01.06.2019.

103 Valtioneuvoston asetus siviilitiedustelusta (29.5.2019/590) vom 29.05.2019, in Kraft getreten am 01.06.2019.

104 Laki tiedustelutoiminnan valvonnasta (121/2019) vom 01.02.2019.

105 Laki henkilötietojen käsittelystä poliisitoimessa (616/2019) vom 01.06.2019, inoffzielle englische Übersetzungen abrufbar unter: https://www.finlex.fi/fi/laki/kaannokset/2019/en20190616_20230209.pdf.

106 Pakkokeinolaki (806/2011) vom 01.01.2014.

107 Vgl. dazu Lohse, Finnish Defence Intelligence Agency - an Actor in National Security?, Journal of Strategic Security Vol. 13, 2/2020 (S. 107-120), 1 (2).

108 Weitere Ausführungen zu den Regelungen der Informationsbeschaffung und -übermittlung durch finnische Nachrichtendienste sind hauptsächlich auf Finnisch zu finden. Eine Übersicht zum finnischen Aufklärungsprozess finnischer Nachrichtendienste ergibt sich aus Lohse, The Intelligence Process in Finland, Scandinavian Journal of Military Studies, Vol. 3, 2020/1, 68 ff., wobei auf die rechtlichen Grundlagen nur vereinzelt näher eingegangen wird.

109 Laki viranomaisten toiminnan julkisuudesta (621/2011) vom 01.12.1999, inoffzielle englische Übersetzungen abrufbar unter: https://www.finlex.fi/fi/laki/kaannokset/1999/en19990621_20150907.pdf.

Polizeigesetzes, Sec. 17 des Gesetzes zur Telekommunikationsüberwachung durch die SUPO oder nach Sec. 79 des Gesetzes zum militärischen Nachrichtendienst möglich. An andere ausländische Nachrichtendienste können finnische Nachrichtendienste Informationen im Sinne einer internationalen Kooperation nach Kapitel 5a Sec. 57 des Polizeigesetzes und nach Sec. 20 des Gesetzes zum militärischen Nachrichtendienst übermitteln.

4. Gezielte Telekommunikationsüberwachung

Maßnahmen der gezielten Telekommunikationsüberwachung (Individualkontrolle) dürfen in Deutschland gemäß §§ 1 Abs. 1 Nr. 1, 3 Abs. 1 G 10 alle nationalen Nachrichtendienste durchführen. Vorausgesetzt ist auf materieller Ebene eine besondere Bedrohungslage für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes.[110] Ferner müssen tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine Straftat aus dem Straftatenkatalog plant, begeht oder begangen hat oder jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind. Die Schwelle der „tatsächlichen Anhaltspunkte“ wurde bereits oben erläutert und bedeutet, dass konkrete und in einem gewissen Umfang verdichtete Umstände vorliegen müssen (näher dazu unter 3.1.1.). Die Telekommunikationsüberwachung nach § 3 Abs. 1 G 10 unterliegt insbesondere einer einfachgesetzlichen Subsidiaritätsklausel dahingehend, dass die Erforschung des jeweiligen Sachverhalts auf andere Weise aussichtslos sein muss (§ 3 Abs. 2 Satz 1 G 10). Des Weiteren gilt gemäß § 3a G 10 ein besonderer Kernbereichsschutz für Inhalte mit höchstpersönlichem Charakter oder aus der Intimsphäre.[111] Die Telekommunikationsüberwachung setzt gemäß § 9 Abs. 3 G 10 formell einen schriftlichen und begründeten Antrag voraus. Im Fall einer Überwachung nach § 3 Abs. 1 G 10 oder nach § 8 Abs. 1 G 10 muss außerdem dargelegt werden, dass der Sachverhalt nicht auf andere Weise erforscht werden kann oder dies jedenfalls nur erschwert möglich wäre. Den Antrag darf nur der jeweilige Behördenleiter oder sein Stellvertreter stellen (§ 9 Abs. 2 G 10). Die Anordnung ergeht schriftlich entweder durch die obersten Landesbehörden oder durch das Bundesministerium des Innern und für Heimat (§ 10 Abs. 1, Abs. 2 G 10).

Im US-amerikanischen Nachrichtendienstrecht richtet sich die individuelle oder gezielte Telekommunikationsüberwachung mit Inlandsbezug durch Nachrichtendienste zur Auslandsaufklärung in erster Linie nach 50 USC §§ 1801 ff. (Elektronische Überwachung, „electronic surveillance“).[112] Diese Regelungen zur elektronischen Überwachung beziehen sich gemäß 50 USC § 1801(f) ausschließlich auf die Beschaffung von Inhalten einer drahtgebundenen oder -losen Kommunikation mittels Überwachungsgeräten einschließlich der Installation und Verwendung dieser Geräte, bei der ein besonderer Bezug zu den USA besteht: Entweder ist das Überwachungsobjekt selbst eine US-Person, also etwa ein US-Staatsangehöriger oder eine Person, die sich

110 Vgl. Löffelmann, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, VI § 4 Rn. 32 f.

111 Vgl. dazu Huber, in: Schenke/Graulich/Ruthig, 2. Aufl. 2018, G 10 § 3a Rn. 6.

112 Vgl. Congressional Research Service, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, 17.03.2023, S. 4.

dauerhaft in den USA aufhält, oder die Überwachung als solches findet in den USA statt.[113] Gezielte Maßnahmen der elektronischen Überwachung setzen gemäß 50 USC § 1804 grundsätzlich eine gerichtliche Anordnung des Foreign Intelligence Surveillance Court (FISC) voraus („court order"). Insoweit müssen diejenigen Stellen, die eine elektronische Überwachung planen, einen entsprechenden Antrag beim FISC stellen. Dieser Antrag muss vor der Antragstellung durch den Attorney General oder seinen Vertreter genehmigt werden und bestimmten formellen Anforderungen genügen. So müssen unter anderem im Antrag diejenigen Tatsachen und Umstände dargelegt werden, die die Annahme begründen, dass die elektronische Überwachung auf eine ausländische Gewalt („Foreign power")[114] oder einen ausländischen Agenten („Agent of a foreign power")[115] gerichtet ist. Ferner muss ein Minimierungsverfahren („Minimization procedures")[116] angegeben werden, das die Beschaffung und Weiterübermittlung von zufällig erlangten Informationen über US-Personen verhindern oder jedenfalls vermeiden sollen.[117] Der FISC prüft den Antrag dahingehend, ob eine Art hinreichender Verdacht („probable cause") vorliegt, dass insbesondere das Überwachungsobjekt entweder eine ausländische Gewalt oder Agent einer ausländischen Gewalt ist und der Ort oder die Einrichtung, auf die die elektronische Überwachung gerichtet ist, wahrscheinlich von diesen Überwachungsobjekten besucht oder genutzt wird (50 USC § 1805(a)(1)).[118] Nicht erforderlich für die Antragstellung ist indes die Darlegung der Gefahr von Straftaten.[119] Nach 50 USC § 1802(a)(1) kann in Ausnahmekonstellationen von der gerichtlichen Anordnung abgesehen werden. Demnach können elektronische Überwachungsmaßnahmen mit einer Dauer von bis zu einem Jahr angeordnet werden, wenn der Präsident dies durch den Attorney General genehmigt ("[…] the President, through the Attorney General, may authorize electronic surveillance without a court order […] if the Attorney General certifies in writing under oath that […]"). Der Attorney General muss schriftlich unter Eid bestätigen, dass erstens die Maßnahme ausschließlich auf die Beschaffung von Inhaltsdaten von Kommunikationsbeziehungen zwischen ausländischen Gewalten oder technischen Informationen in Bezug auf eine ausländische Gewalt gerichtet ist und zweitens mit hinreichender Wahrscheinlichkeit („substantial likelihood") davon ausgegangen werden kann, dass keine Kommunikation überwacht wird, bei der eine US-Person teilnimmt. Keine elektronische Überwachung im Sinne des 50 USC §§ 1801(f), 1802 liegt indes vor, wenn die Beschaffung nicht innerhalb der USA stattfindet, auf eine Person gerichtet ist, die keine US-Person ist, und diese sich nicht in den USA aufhält. Letzteres unterfällt vielmehr den besonderen Anforderungen des 50 USC § 1881a („Targeting certain persons

113 Zur Definition 50 USC § 1801(i); Congressional Research Service, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, 17.03.2023, S. 3.

114 Zur Definition 50 USC § 1801(a).

115 Zur Definition 50 USC § 1801(b).

116 Zur Definition 50 USC § 1801(h).

117 Vgl. im Einzelnen dazu Congressional Research Service, Foreign Intelligence Surveillance Act (FISA): An Overview, 06.04.2021; siehe ferner erläuternd dazu, Office of the Director of National Intelligence, Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act, 2017, S. 4.

118 Vgl. Congressional Research Service, Foreign Intelligence Surveillance Act (FISA): An Overview, 06.04.2021.

119 Bureau of Justice Assistance, The Foreign Intelligence Surveillance Act of 1978 (FISA).

outside the United States other that United States persons“).[120] Anders als bei den übrigen im FISA geregelten Überwachungsmaßnahmen kann dies zusammen durch den Attorney General und den DNI für eine Dauer bis zu einem Jahr genehmigt werden. Dem FISC soll grundsätzlich vor der Durchführung der Maßnahme die schriftliche Genehmigung zur Verfügung gestellt werden, außer es ist aus Dringlichkeitsgründen nicht möglich, sodass dem FISC so schnell wie möglich nach Beginn der Durchführung die Genehmigung nachzureichen ist (50 USC § 1881(h)(1)). Der FISC prüft in diesem Zusammenhang allerdings nur formelle Anforderungen der Maßnahme (50 USC § 1881a(j)).[121] 50 USC §§ 1881b, 1881c regeln wiederum die Überwachung von US-Personen außerhalb der USA und legen insoweit fest, dass der FISC einen hinreichenden Verdacht prüfen muss (50 USC § 1881b(c)(B), 50 USC § 1881c(c)(B)).

Das französische Nachrichtendienstrecht ermächtigt die französischen Nachrichtendienste durch Art. L852-1 CSI, zum Zwecke der Verteidigung und Stärkung nationaler Interessen im Sinne von Art. L811-3 CSI elektronische Kommunikation zu überwachen. Voraussetzung der Anordnung einer solchen Maßnahme ist die Genehmigung durch den Premierminister nach Art. L821-1 CSI: Um eigenmächtige Handlungen der Nachrichtendienste auszuschließen, muss der Nachrichtendienst, der bestimmte Kommunikationen überwachen möchte, über sein jeweils zuständiges Ministerium und den jeweils zuständigen Minister einen schriftlichen und begründeten Antrag mit Angabe der Einzelheiten der Überwachung einbringen (Art. L821-2 CSI), den der Premierminister genehmigt.[122] Bevor der Premierminister den Antrag genehmigt, wird dieser der Nationalen Kommission zur Kontrolle nachrichtendienstlicher Maßnahmen („Commission nationale de contrôle des techniques de renseignement“) übermittelt, der innerhalb von 24 Stunden eine Stellungnahme zum Antrag abgibt (Art. L821-3 CSI). Der Premierminister ist an die Stellungnahme der Nationalen Kommission zwar nicht gebunden. Jedoch muss er die Angelegenheit im Fall der Ablehnung der Stellungnahme dem Staatsrat („Conseil d'Etat“) vorlegen, der darüber zu entscheiden hat.[123] Außerdem ist gemäß Art. L852-1 VI geregelt, dass der Premierminister nach Rücksprache mit der Nationalen Kommission die genehmigten Überwachungsmaßnahmen auf eine maximale Anzahl begrenzt, um so vor der Genehmigung neuer Überwachungsmaßnahmen nicht mehr erforderliche Überwachungsmaßnahmen zu beenden.[124]

Nach Sec. 15 IPA 2016 sieht auch das britische Nachrichtendienstrecht eine gezielte Überwachung von Telekommunikationen unter anderem von einzelnen Personen oder bestimmten Gruppen von Personen auf der Grundlage eines entsprechenden Antrags vor (Sec. 15(1)(a), (2), Sec. 17 IPA 2016). Sec. 18(1) IPA 2016 zählt insoweit die zuständigen Stellen auf, die Anordnungen beantragen dürfen. Ein Secretary of State – der mit einem Bundesminister vergleichbar ist – ordnet

120 Vgl. dazu auch Congressional Research Service, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, 17.03.2023, S. 9.

121 Vgl. Congressional Research Service, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, 17.03.2023, S. 10.

122 Warusfel, The new French intelligence law, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 133; .

123 Vgl. zur „blocking” Entscheidung, European Union Agency for Fundamental Rights, Surveillance by Intelligence Services - Fundamental Rights Safeguards and Remedies in the EU - 2023 Update, 2023, S. 13.

124 Wetzeling/Vieth, Massenüberwachung bändigen, 2019, S. 53.

die Überwachung der Telekommunikation an („Power of Secretary of State to issue warrants“, Sec. 19 IPA 2016). Das Gesetz unterscheidet zwischen unterschiedlichen Formen von Anordnungen: Überwachungsanordnung („targeted interception warrant“), Überprüfungsanordnung „targeted examination warrant“ und Rechtshilfeanordnung („mutual assistance warrants“).[125] Der Secretary of State prüft vor allem, ob die jeweilige Anordnung im Einzelfall erforderlich („necessary“) und verhältnismäßig („proportionate“) ist. Die Überwachungs- und Überprüfungsanordnung ist nach Sec. 20(2) IPA in der Regel erforderlich, wenn sie 2016 im Interesse der nationalen Sicherheit oder zur Vermeidung oder Aufdeckung schwerwiegender Straftaten notwendig ist.[126] Wenn Informationen im Interesse des wirtschaftlichen Wohlstandes des UK beschafft werden sollen, ist insoweit zu berücksichtigen, dass nach Sec. 20(4) IPA 2016 eine Anordnung nur zulässig ist, wenn sich die erforderlichen Informationen auf Handlungen oder Bestrebungen von Personen außerhalb des UK beziehen. Ferner legt Sec. 20(5) IPA 2016 fest, dass eine Anordnung nicht als erforderlich anerkannt werden soll, wenn dadurch nur Erkenntnisse und Beweise für Gerichtsverfahren („legal proceedings“) gewonnen werden sollen. Als allgemeine Vorgabe sind außerdem nach Sec. 2(2) RIPA 2016 alle genehmigenden öffentlichen Stellen verpflichtet, die Maßnahme dahingehend zu prüfen, ob es eine weniger eingriffsintensive Maßnahme für die Informationen gibt, ein höheres Maß an Schutz sensibler Informationen angewendet werden sollte und das öffentliche Interesse am Schutz der Integrität und Sicherheit der Kommunikation und ein etwaiges anderes Schutzinteresse der Privatsphäre berücksichtigt ist.

Das niederländische Nachrichtendienstrecht regelt die gezielte Telekommunikationsüberwachung nach Art. 47 Wiv 2017. Die Maßnahme setzt eine Genehmigung des zuständigen Ministers auf Antrag des Leiters des jeweiligen Nachrichtendienstes voraus (Abs. 2). Außerdem gelten allgemeine Anforderungen an einen Antrag für die Erteilung einer Sondermaßnahme (Art. 29 Wiv 2017). Zudem müssen im Antrag besondere Angaben gemacht werden, unter anderem zu den Gründen, nach denen die jeweilige Maßnahme notwendig (Buchstabe f) sowie verhältnismäßig zum Zweck der Maßnahme (Buchstabe i) ist und keine mildere Maßnahme möglich wäre (Buchstabe j). Zum anderen wird besonders für die Telekommunikationsüberwachung festgelegt, dass unter anderem die Zielperson oder -organisation näher bestimmt werden muss (Art. 47 Abs. 3 Wiv 2017).

Zu den gesetzlichen Anforderungen der gezielten Telekommunikationsüberwachung in Finnland finden sich kaum deutsch- oder englischsprachige Ausführungen.[127] Die vorliegenden Informationen beruhen auf den Ausführungen Finnlands nach einer Anfrage der Wissenschaftlichen Dienste des Deutschen Bundestages. Sowohl der zivile Nachrichtendienst SUPO als auch der

---

125 Ausführlich dazu McKay/Walker, Intelligence law in the United Kingdom, in: Dietrich/Gärditz/Graulich et al., Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 123 f.

126 Verfahrensmäßige Besonderheiten gelten bei „schottischen Anträgen“, vgl. dazu Sec. 19(4)(a), Sec. 21 und Sec. 22 IPA 2016.

127 Vgl. zum finnischen Recht und einer Unterscheidung zwischen der nationalen und internationalen Telekommunikationsüberwachung die Ausführungen des Office of the Assistant Attorney General, Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086, S. 18 Fn. 12. Demnach soll bei nationaler Telekommunikation, die innerhalb Finnlands stattfindet, die SUPO für die Überwachung nach dem Polizeigesetz (Kapitel 5a §§ 3-4), und bei internationalen Telekommunikationen, bei der ein Kommunikationsteilnehmer im Ausland ist, der militärische Nachrichtendienst nach dem Gesetz zum militärischen Nachrichtendienst (§§ 12, 68-71) zuständig sein.

militärische Nachrichtendienst darf die Telekommunikation überwachen. Für alle nachrichtendienstlichen Maßnahmen gilt, dass insbesondere die Grund- und Menschrechte, der Verhältnismäßigkeitsgrundsatz und der Grundsatz des geringsten Eingriffs zu beachten sind (Kapitel 1 Sec. 2-5, Kapitel 5a Sec. 4 des Polizeigesetzes; Sec. 1, 4, 7 und 9 des Gesetzes zur Telekommunikationsüberwachung durch die SUPO; Sec. 5-9 und 12 des Gesetzes zum militärischen Nachrichtendienst). Die gezielte Telekommunikationsüberwachung darf nicht ohne Grund wegen personenbezogener Merkmale, wie unter anderem Alter, Geschlecht, Herkunft, Nationalität, Wohnort, Sprache oder Religion durchgeführt werden. Zudem ist eine Voraussetzung der gezielten Telekommunikationsüberwachung, dass diese notwendig ist, um Informationen über Tätigkeiten zu erlangen, die die nationale Sicherheit schwerwiegend gefährden. Die Informationen dürfen zudem nicht auf andere Weise erlangt werden können. Die wesentlichen Vorschriften, die die Telekommunikationsüberwachung durch die SUPO regeln, sind Kapitel 5a Sec. 6 und 7 des Polizeigesetzes und Sec. 7 und 9 des Gesetzes zur Telekommunikationsüberwachung durch die SUPO. Demnach entscheidet ein Gericht über die Maßnahme auf Antrag der SUPO. Die Maßnahme kann jeweils für bis zu sechs Monate angeordnet werden und, wenn eine natürliche Person überwacht wird, für bis zu drei Monate. Die Telekommunikationsüberwachung durch den militärischen Nachrichtendienst erfolgt auf der Grundlage von Sec. 34 des Gesetzes zum militärischen Nachrichtendienst. Das Verfahren richtet sich nach Sec. 36 des Gesetzes zum militärischen Nachrichtendienst.

***