Xenia Lang

Geheimdienstinformationen im deutschen und amerikanischen Strafprozess

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

Strafrechtliche Forschungsberichte

Herausgegeben von Ulrich Sieber

in Fortführung der Reihe
„Beiträge und Materialien aus dem Max-Planck-Institut
für ausländisches und internationales Strafrecht Freiburg“
begründet von Albin Eser

Band S 145

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Geheimdienstinformationen im deutschen und amerikanischen Strafprozess

Xenia Lang

Duncker & Humblot · Berlin

Bibliografische Information der Deutschen Nationalbibliothek

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

DOI https://doi.org/10.30709/978-3-86113-811-2

Umschlagbild: Frank Schmidt, Köln
Foto der Autorin: Baschi Bender
Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim
Printed in Germany

ISSN 1860-0093
ISBN 978-3-86113-811-2 (Max-Planck-Institut)
ISBN 978-3-428-14622-2 (Duncker & Humblot)
Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2013 von der Rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg als Dissertation angenommen. Gesetzgebung, Literatur und Rechtsprechung sind bis April 2013 berücksichtigt.

Die Arbeit entstand während meiner Zeit als Doktorandin am Max-Planck-Institut für ausländisches und internationales Strafrecht im Rahmen der International Max Planck Research School for Comparative Criminal Law (IMPRS-CC). An dieser Stelle möchte ich allen danken, die mich bei meiner Promotion unterstützt haben.

Meinem Doktorvater Herrn Prof. Dr. Dr. h.c. mult. *Ulrich Sieber* gilt mein herzlicher Dank für die Begleitung der Promotion und die mir gewährte Möglichkeit, an internationalen Konferenzen in Deutschland, der Türkei und den USA teilzunehmen. Erst der Zugang zu den ausgezeichneten Arbeitsbedingungen am Max-Planck-Institut hat mir die Erstellung der Arbeit ermöglicht.

Des Weiteren bedanke ich mich bei Herrn Prof. Dr. Dr. h.c. *Hans-Jörg Albrecht* für die zügige Erstellung des Zweitgutachtens.

Frau *Ines Hofmann* danke ich für die exzellente redaktionelle Betreuung sowie die angenehme Zusammenarbeit.

Ganz besonders danke ich schließlich meinen Eltern *Lieselotte* und *Bernd Lang* für ihre vorbehaltlose liebevolle Unterstützung, meinem Bruder *Alexander Lang* für seine stets klaren Worte und meinem Freund *Alexander Schumm* für seine fortwährende Geduld und Motivierung.

Frankfurt, August 2014 *Xenia Lang*

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	andere Ansicht
Abb.	Abbildung
Abs.	Absatz
Abk.	Abkürzung
a.E.	am Ende
a.F.	alte Fassung
AG	Amtsgericht
Alt.	Alternative
Am. Crim. L. Rev.	American Criminal Law Review
Am. J. Comp. L.	American Journal of Comparative Law
Am. J. Int'L.	American Journal of International Law
Anh.	Anhang
Annu. Rev. Law. Soc. Sci.	Annual Review of Law and Social Science
AnwBl	Anwaltsblatt
Army Law.	Army Lawyer
Art.	Artikel
ATD	Antiterrordatei
Aufl.	Auflage
AUMF	Authorization to Use Military Force
Az.	Aktenzeichen
BbgVerfG	Verfassungsgericht des Landes Brandenburg
B. C. L. Rev.	Boston College Law Review
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten

BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMVg	Bundesministerium der Verteidigung
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BT-Drs.	Bundestagsdrucksache
B.U. Int'l L.J.	Boston University International Law Journal
B.U. Pub. Int. L.J.	Boston University Public Interest Law Journal
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz)
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa
Cal. L. Rev.	California Law Review
Ch.	Chapter
CIA	Central Intelligence Agency
CIPA	Classified Information Procedures Act
Colum. J. Transnat'l L.	Columbia Journal of Transnational Law
COMINT	Communications Intelligence
CLPO	Civil Liberties Protection Officer
Crim. L. Rev.	Criminal Law Review
CRS	Congressional Research Service
CTC	Counter Terrorism Center
d.h.	das heißt
DHS	Department of Homeland Security
DI	Domestic Intelligence
DIA	Defense Intelligence Agency
DII	Domestic Intelligence Investigation
DJT	Deutscher Juristentag
DNI	Director of National Intelligence
DöV	Die Öffentliche Verwaltung

DRiZ	Deutsche Richterzeitung
DStR	Deutsches Steuerrecht
DVBl	Deutsches Verwaltungsblatt
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
Einl.	Einleitung
EJCCL & CJ	European Journal of Crime Criminal Law and Criminal Justice
EMRK	Europäische Konvention zum Schutz der Menschenrechte
E.O.	Executive Order
Eur. J. L. Reform	European Journal of Law Reform
f., ff.	folgende, fortfolgende
FBI	Federal Bureau of Investigation
Fed. Reg.	Federal Register
FI	Foreign Intelligence
FII	Foreign Intelligence Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
Fn.	Fußnote
FRCrimP	Federal Rules of Criminal Procedure
FRE	Federal Rules of Evidence
G10	Gesetz zur Neuregelung und Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GA	Goltdammer's Archiv für Strafrecht
GBA	Generalsbundesanwalt
Geo. L. J.	Georgetown Law Journal
Geo. Wash. L. Rev.	George Washington Law Review
Gestapo	Geheime Staatspolizei
GG	Grundgesetz
ggf.	gegebenenfalls
GIZ	Gemeinsames Internetzentrum
GLJ	German Law Journal
GTAZ	Gemeinsames Terrorabwehrzentrum
GVG	Gerichtsverfassungsgesetz
Harv. J. L. & Pub. Pol'y	Harvard Journal of Law and Public Policy
Harv. J. Leg.	Harvard Journal of Legislation

Harv. NSJ	Harvard National Security Journal
HPSCI	House Permanent Select Committee on Intelligence
HRRS	Höchstrichterliche Rechtsprechung im Strafrecht
Hrsg.	Herausgeber
Hs.	Halbsatz
HUMINT	Human Source Intelligence
I&A	Office of Intelligence and Analysis
IC	Intelligence Community
IJIC	International Journal of Intelligence and Counterintelligence
Int'l; Int.	International
Int'l Legal Persp.	International Legal Perspectives
ISE	Information Sharing Environment
I/S: J.L. & Pol'y for Info. Soc'y	I/S: A Journal of Law and Policy for the Information Society
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
J.	Journal
JA	Juristische Arbeitsblätter
J. Nat'l Sec. L. & Pol'y	Journal of National Security Law and Policy
JR	Juristische Rundschau
JTTF	Joint Terrorism Task Forces
JURA	Juristische Ausbildung
JuS	Juristische Schulung
JZ	Juristenzeitung
KK	Karlruher Kommentar
KritJ	Kritische Justiz
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
KSA	Kommando Strategische Aufklärung
LEC	Law Enforcement Community
LfV	Landesämter für Verfassungsschutz
lit.	littera
L. J.	Law Journal
Loy. U. Chi. L. J.	Loyola University of Chicago Law Journal
L. Rev.	Law Review
MAD	Militärischer Abschirmdienst

MADG	Gesetz über den Militärischen Abschirmdienst
MC	Military Commission
MCA	Military Commission Act
Mich. L. Rev.	Michigan Law Review
MilNWBw	Militärisches Nachrichtenwesen der Bundeswehr
MLR	Modern Law Review
MMR	Multimedia und Recht
MüKoStGB	Münchner Kommentar zum Strafgesetzbuch
m.w.N.	mit weiteren Nachweisen
NCS	National Clandestine Service
NCTC	National Counter Terrorism Center
NGA	National Geospatial-Intelligence Agency
NIS	National Intelligence Strategy
NISS	National Intelligence Sharing Strategy
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
No.	Number
Nr.	Nummer
NRO	National Reconnaissance Office
NSA	National Security Agency
NSDAP	Nationalsozialistische Deutsche Arbeiterpartei
NSL	National Security Letter
NSS	National Security Strategy
NStZ	Neue Zeitschrift für Strafrecht
NULR	Northwestern University Law Review
NVwZ	Neue Zeitschrift für Verwaltungsrecht
N.Y.U. J.L. & Liberty	New York University Journal of Law & Liberty
ODNI	Office of the Director of National Intelligence
OK	Organisierte Kriminalität
OVG	Oberverwaltungsgericht
PKGr	Parlamentarisches Kontrollgremium
PKGrG	Kontrollgremiumsgesetz
Pub. L.	Public Law
RAF	Rote Armee Fraktion
RIDP/IRPL	Revue Internationale de Droit Pénal/International Review of Penal Law

RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
Rn.	Randnummer
S.	Seite
SAC	Special Agent in Charge
SächsVerf	Verfassung des Freistaates Sachsen
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SAIS Review	School of Advanced International Studies Review
SAM's	Special Administrative Measures
S. Cal. L. Rev.	Southern California Law Review
S. Ct.	Supreme Court
SD	Sicherheitsdienst
SIGINT	Signals Intelligence
SJC	Senate Judiciary Committee
SK	Systematischer Kommentar
sog.	sogenannte(r)
SS	Schutzstaffel
SSCI	Senate Select Committee on Intelligence
Stan. L. & Pol'y Rev.	Stanford Law & Policy Review
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
str.	strittig
StraFo	Strafverteidigerforum
StV	Strafverteidiger
Tex. L. Rev.	Texas Law Review
TKÜ	Telekommunikationsüberwachung
Tul. L. Rev.	Tulane Law Review
Tul. J. Comp. & Int'l L.	Tulsa Journal of Comparative and International Law
UCA	Undercover Agent
U. Chi. L. Rev.	University of Chicago Law Review
UCLA	University of California at Los Angeles
UCLA J. Int'l L. & For. Aff.	UCLA Journal of International Law and Foreign Affairs
U. Colo. L. Rev.	University of Colorado Law Review
U. Pa. L. Rev.	University of Pennsylvania Law Review
U.S.	United States
U.S.C.	United States Code

ü.A.	überwiegende Ansicht
Val. U. L. Rev.	Valparaiso University Law Review
Vand. L. Rev.	Vanderbilt Law Review
Var.	Variante
VE	Verdeckter Ermittler
vgl.	vergleiche
Vill. L. Rev.	Villanova Law Review
Vol.	Volume
Vor	Vorbemerkungen
VwVfG	Verwaltungsverfahrensgesetz
wistra	Zeitschrift für Wirtschaft, Steuer und Strafrecht
Yale L.J.	Yale Law Journal
Yale L. & Pol'y Rev.	Yale Law & Policy Review
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
z.B.	zum Beispiel
ZFdG	Gesetz über das Zollkriminalamt und die Zollfahndungsämter
ZFIS	Zeitschrift für Innere Sicherheit in Deutschland und Europa
ZfRV	Zeitschrift für Rechtsvergleichung
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZKA	Zollkriminalamt
ZNBw	Zentrum für das Nachrichtenwesen der Bundeswehr
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

Teil 1

Einleitung und Grundlagen des Rechtsvergleichs

I. Gegenstand, Ziel und Methode der Untersuchung

Die effektive Zusammenarbeit der verschiedenen Sicherheitsbehörden ist ein notwendiges Mittel zur Erfüllung des staatlichen Schutzauftrags und zur Gewährleistung innerer Sicherheit. Undurchsichtige Kriminalitätsstrukturen und asymmetrische Konfliktlagen steigern den staatlichen Informationsbedarf und geben Forderungen nach umfassenden Überwachungskonzepten Vorschub. In diesem Prozess spielt die Informationsgewinnung durch Geheim- und Nachrichtendienste eine entscheidende Rolle.[1] Weitreichende Ermittlungsbefugnisse erlauben den Geheimdiensten den Zugriff auf Informationen, die anderen Behörden verschlossen bleiben. Neben präventiven Einsatzmöglichkeiten wird vermehrt die Nutzung von Geheimdienstinformationen auch zu repressiven Zwecken diskutiert. Insbesondere wenn eine Aburteilung nur auf der Grundlage geheimdienstlichen Wissens möglich erscheint, besteht vonseiten der Strafverfolgungsbehörden ein vitales Interesse an einem Wissensaustausch. Da Geheimdienstinformationen jedoch nicht mit Blick auf ein Strafverfahren erhoben werden, sind sie nicht unreflektiert als Beweismittel nutzbar. Unterschiedliche Erhebungsstandards, Kompetenzfragen und Rechte der Betroffenen können vielmehr der Einführung geheimdienstlich beschaffter Erkenntnisse in das Strafverfahren entgegenstehen. Die besondere Brisanz einer Kooperation mit den Nachrichtendiensten wurde vom Bundesverfassungsgericht zuletzt in seinem Urteil zur Antiterrordatei vom 24. April 2013 herausgestellt.[2] Ebenfalls im Jahr 2013 verdeutlichte der NSA-Skandal die Befürchtungen, die mit einer (zu) umfassenden Datenerhebung durch die Geheimdienste verbunden sind. Aber auch innerhalb des Strafverfahrens kann es zu gravierenden Interessenskonflikten kommen, wenn nationale Sicherheitsinteressen eine (vollständige) Offenlegung und damit strafprozessuale Nutzung geheimdienstlichen Wissens erschweren.

Die bei einer Nutzung von Geheimdienstinformationen aufeinandertreffenden Freiheits-, Sicherheits-, Strafverfolgungs- und Geheimhaltungsinteressen stellen das Strafrecht vor erhebliche Herausforderungen.[3] Zur Diskussion steht vor allem,

---

[1] Vgl. *Schäuble,* ZRP 2007, S. 211.

[2] Siehe BVerfG, 1 BvR 1215/07 vom 24.4.2013.

[3] Die vorliegende Arbeit wurde im Rahmen des langfristig angelegten Forschungsprogramms der *Research School for Comparative Criminal Law* der strafrechtlichen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht erstellt, das

ob und wie geheimdienstliche Erkenntnisse nach erfolgter oder versuchter Verwirklichung eines Straftatbestands als Beweismittel in einem Strafverfahren herangezogen werden können. Die besondere Relevanz dieser Thematik wird an Terrorverfahren, wie etwa gegen *Motassadeq* in Deutschland und *Moussaoui* in den USA, deutlich. In diesen Strafverfahren wurde über mehrere Instanzen hinweg um eine wirksame Aburteilung gerungen.[4] Die in den Verfahren zutage getretenen Unsicherheiten sind gerade bei gravierenden Strafandrohungen nicht akzeptabel. Die strafprozessuale Handhabung von Geheimdienstinformationen bedarf demzufolge einer eingehenden Untersuchung.

Die beschriebene Problematik stellt sich auch in anderen Rechtsordnungen. Insbesondere die USA haben mit ihrer Erklärung des *war on terror* neue Maßstäbe beim Einsatz geheimdienstlicher Überwachungsmaßnahmen zur Terrorismusbekämpfung gesetzt. Dort kam es vor allem nach den Anschlägen vom 11. September 2001 zu zahlreichen Reformen, die eine verstärkte Terrorabwehr und erleichterte Aburteilung terroristischer Akteure zum Ziel hatten. Aus europäischer Perspektive zeichnen sich die dort verfolgten Ansätze durch ihre besondere Radikalität sowie durch eine überraschende Transparenz aus.[5] Diese Besonderheiten führen zusammen mit der andersartigen Strukturierung des Geheimdienstsektors und der adversatorischen Prägung des Strafverfahrens zu einem vom deutschen Recht abweichenden Lösungsmodell. Der Vergleich der in beiden Rechtsordnungen angebotenen Lösungskonzepte ist aufgrund der erheblichen Relevanz dieser Thematik notwendig, um den Blick auf das deutsche Lösungsmodell zu schärfen.[6] Insbesondere die potentiell aktivere Rolle der Verfahrensbeteiligten könnte sich in Bezug auf das deutsche Lösungsmodell als hilfreicher Impuls auswirken. Umgekehrt sind mit der Wahl des amerikanischen Rechts als Vergleichsmaßstab besondere Herausforderungen verbunden. Der im amerikanischen Recht zentrale Begriff *intelligence* ist keineswegs auf geheimdienstliche Informationen begrenzt, sondern kann sich auf eine Behörde, den Prozess der Informationsverarbeitung sowie das Ergebnis eines Analyseprozesses beziehen. Diese begriffliche Vielschichtigkeit erschwert die Identifizierung der als „Geheimdienste“ bezeichneten Institutionen.

Forschungsziel ist die Herausarbeitung des deutschen und amerikanischen Grundmodells bei der Nutzung von Geheimdienstinformationen im Strafprozess. Bei der Bewältigung dieser Aufgabe orientiert sich die Arbeit an zwei übergeordneten Problemkreisen. Zum einen wird untersucht, inwiefern sich die abweichenden Lösungsmodelle auf Unterschiede in der Sicherheitsarchitektur zurückführen

---

sich unter anderem den funktionalen Grenzen des Strafrechts widmet. Vgl. zum Forschungsprogramm *Sieber,* ZStW 119 (2007), S. 1ff.

[4] BGH 3 StR 218/03, Urteil vom 4.3.2004; *United States v. Moussaoui*, 591 F.3d 263 (4th Cir. 2010).

[5] Vertiefend *Jäger/Daun,* in: Borchert, S. 61.

[6] Zu diesem Vorteil eines Rechtsvergleichs siehe u.a. *King,* Int’l Legal Persp. (12) 2002, S. 186; *Rheinstein/von Borries/Niethammer,* S. 26, jeweils m.w.N.

lassen. Zum anderen werden die Auswirkungen nationaler Sicherheitsinteressen auf die Nutzung und Offenlegung von Geheimdienstinformationen im Strafprozess analysiert. Die Aufarbeitung erfolgt anhand von Einzelfragen:

- Wie ist das Verhältnis der Geheimdienste zu den Strafverfolgungsbehörden?
- Welche Auswirkungen hat dieses Verhältnis auf die Informationserhebung und den Informationsaustausch? Findet eine Informationsübermittlung an den Strafverfolgungssektor statt und falls ja, wie?
- Gestattet das Rechtssystem die Nutzung von Geheimdienstinformationen zur Strafverfolgung? Falls ja, unter welchen Voraussetzungen? Falls nein, erfolgt ein Umweg über andere, punitiv wirkende außerstrafrechtliche Verfahrensarten, die ein funktionales Äquivalent zum Strafverfahren darstellen?
- Unter welchen Voraussetzungen können nationale Sicherheitsinteressen als Geheimhaltungsgrund im Strafverfahren herangezogen werden? Gegenüber wem, wann und wie ist eine Geheimhaltung zulässig?
- Werden die Nachteile einer (partiellen) Geheimhaltung kompensiert? Falls ja, wie?

Anhand dieser Fragen sind die Grundlinien und Ursachen der nationalen Modelle herauszuarbeiten sowie deren Möglichkeiten und Grenzen auszuloten. Der Rechtsvergleich soll hierbei ein besseres Verständnis der deutschen Rechtsordnung ermöglichen und neue Denkanstöße für die Entwicklung und Reform des deutschen Rechts liefern.

Methodisch wird ein funktionaler Vergleich des deutschen und amerikanischen Rechts vorgenommen. Den begrifflichen Vielschichtigkeiten begegnet die vorliegende Arbeit mit der Erarbeitung einer eigenständigen Definition. Die Begriffe „Geheimdienste“ und „Geheimdienstinformation“ werden anhand wichtiger Identifikationsmerkmale präzisiert und damit den Belangen der vorliegenden Arbeit angepasst. Schwierigkeiten ergeben sich aufgrund der in diesem Bereich defizitären Quellenlage.[7] Diese ist der besonderen Sensibilität und Verschlossenheit des Geheimdienstsektors sowie dem in Sicherheitsfragen bestehenden Reformeifer des Gesetzgebers geschuldet. In den vergangenen Jahrzehnten wurde das Sicherheits- und Geheimdienstwesen national wie international zahlreichen Reformen unterworfen. Beginnend mit den Herausforderungen des Kalten Krieges über die Zunahme des internationalen Drogenhandels und der Organisierten Kriminalität bis

---

[7] Zu diesem Problem vgl. *König,* S. 44f. Zudem fokussiert sich der wissenschaftliche Diskurs regelmäßig auf Teilaspekte oder auf die Rechtslage vor 2008, so unter anderem *Frister,* FS für Bemmann, S. 348ff; *Roggan,* Polizeistaat, S. 30ff; *Lisken/Denninger,* in: Lisken/Denninger/Rachor, S. 118; *Soiné,* NStZ 2007, S. 247ff; *Zöller,* in: Roggan/Kutscha, S. 447. Zur neueren Rechtslage lediglich *Rehbein,* S. 19; *Knieriem,* StV 2008, S. 601; *Singelnstein,* ZStW 120 (2008), S. 878 Fn. 118. Ebenfalls lückenhaft sind die Erläuterungen in der BT-Drs. 16/5846, S. 64. Ohne Berücksichtigung der aktuellen Rechtslage vgl. *Engelhart,* in: Wade/Maljević, S. 528ff; *Nagler,* in: Baden-Württembergische Strafverteidiger e.V., S. 164.

hin zum internationalen Terrorismus hat das Recht zahlreiche Neuerungen erfahren. Diese Reformbewegungen konnten von Literatur und Rechtsprechung bislang nur schrittweise und unvollständig aufgearbeitet werden. Die für die Behandlung der vorliegenden Problematik erreichbaren Informationen sind dementsprechend dürftig. Diese Lücke versucht die vorliegende Arbeit unter Rückgriff auf das deutsche und amerikanische Gesetzesrecht,[8] die vereinzelt einschlägigen Untersuchungen in Literatur und Rechtsprechung sowie durch offizielle Informationen vonseiten der Dienste zu schließen. Der defizitäre Forschungsstand rechtfertigt zugleich die Auseinandersetzung mit der Thematik und damit die Existenz der vorliegenden Arbeit.

Die Darstellung gliedert sich in fünf Teile. Im ersten Teil wird der dieser Arbeit zugrunde liegende Begriff der Geheimdienstinformation inhaltlich präzisiert. Im zweiten und dritten Teil folgen die Landesberichte, welche sich ihrerseits in einen allgemeinen und einen besonderen Teil aufgliedern. Der allgemeine Teil erläutert zunächst relevante Aspekte der nationalen Verfahrensordnungen und gibt einen Überblick über die jeweiligen Produzenten von „Geheimdienstinformationen". In dem sich anschließenden besonderen Teil werden die beiden eigentlichen Problemkreise bei der Nutzung von Geheimdienstinformationen im Strafprozess erörtert. Zuerst wird die Verortung der Geheimdienste in die nationale Sicherheitsarchitektur, die Besonderheiten geheimdienstlicher Ermittlungen im Vergleich zu Ermittlungen der Strafverfolgungsbehörden sowie die jeweiligen Grenzen und Konsequenzen für den Informationsaustausch und die Beweisverwertung dargelegt. Danach werden die im Strafverfahren anwendbaren Geheimhaltungs- und Kompensationsregeln zum Schutz nationaler Sicherheitsinteressen vorgestellt. Die Geheimhaltungsproblematik wird dabei anhand verschiedener Geheimhaltungsstrategien durchgespielt. Im vierten Teil werden die Erkenntnisse des deutschen und amerikanischen Landesberichts vergleichend gegenübergestellt. Der fünfte Teil schließt die Arbeit mit einer Schlussbetrachtung ab.

II. Definition von „Geheimdienstinformationen"

Grundlage eines Rechtsvergleichs ist zunächst die Frage, *was* verglichen werden soll. Ausgehend vom Arbeitstitel steht die Nutzung des als „Geheimdienstinformation" bezeichneten Wissens im Zentrum der Analyse. Im Gegensatz zu anderen Begriffen hat der der Geheimdienstinformation den entscheidenden Vorteil, dass er unmittelbare Assoziationen zu einem bestimmten Sicherheitssektor weckt.[9] Meist

---

[8] Das Informationsdefizit wirkt sich diesbezüglich nur mittelbar aus, da vor allem der aktuelle Rechtszustand aufgearbeitet werden soll. Dieser ist in der Regel offen zugänglich.

[9] Vgl. *Rehbein,* S. 24. Dies ist in Bezug auf nachrichtendienstliche Erkenntnisse oder den englischen Begriff *intelligence* nicht zwingend der Fall.

wird dabei eine unmittelbare Verbindung zu verdeckt operierenden Agenten, Gegenspionage und zweifelhaften Ermittlungsmethoden gezogen. Weniger eindeutig ist allerdings, was in rechtlicher Hinsicht unter diesen Begriff gefasst werden soll. Gerade im deutschen Kontext ist die Bezeichnung einer Institution als Geheimdienst problematisch. Hier wird die Bezeichnung „Nachrichtendienst“ oder „Verfassungsschutzbehörde“ bevorzugt.[10] Diese beiden letztgenannten Begrifflichkeiten lassen sich allerdings nicht ohne Weiteres auf die amerikanische Rechtsordnung übertragen. In den USA ist die vielschichtige Bezeichnung *intelligence* vorherrschend, die ebenfalls keine eindeutige Entsprechung im deutschen Recht findet. Zur Ermöglichung eines funktionalen Rechtsvergleichs müssen daher zunächst die Begrifflichkeiten im nationalen Kontext geklärt und für die Belange der vorliegenden Arbeit präzisiert werden. Hierzu müssen drei Fragenkomplexe beantwortet werden. Erstens: Was wird allgemein unter Geheimdiensten beziehungsweise Geheimdienstinformationen und *intelligence* verstanden? Zweitens: Welche anderen Begriffe sind in den jeweiligen Rechtsordnungen einschlägig und gegebenenfalls vorzugswürdig? Drittens: Welche Begriffe und welches funktionale Verständnis werden der vorliegenden Arbeit zugrunde gelegt?

Die Beantwortung dieser Fragen bildet den Grundstein der rechtsvergleichenden Analyse. Erst wenn Einigkeit darüber besteht, welches funktionale Verständnis im Kern der Untersuchung zugrunde liegt, kann ein sinnvoller Rechtsvergleich durchgeführt werden. Im Folgenden werden daher die im deutschen und amerikanischen Recht relevanten Begrifflichkeiten in Grundzügen dargestellt. Im Anschluss daran wird der Begriff der Geheimdienstinformation für die Zwecke der vorliegenden Arbeit anhand wichtiger Identifikationsmerkmale präzisiert.

A. Begrifflichkeiten im nationalen und historischen Kontext

Die nachfolgenden Ausführungen geben einen Überblick über die im deutschen und amerikanischen Geheimdienstwesen zentralen Begriffe. Diese bilden die Grundlage für die sich daran anschließende eigenständige Begriffsbestimmung.

1. Deutschland

Im deutschen Kontext wohl am prominentesten ist die Bezeichnung „Geheimdienste“. In der einschlägigen Literatur werden von der Definition des Geheimdienstes ständige staatliche Einrichtungen erfasst, welche politisch, militärisch oder wirtschaftlich bedeutsame Informationen sammeln und auswerten sowie unmittel-

---

[10] Vgl. *Singer,* OK, S. 11, der eine Bezeichnung als Geheimdienste als „unredlich“ empfindet. Zur Begründung verweist er auf das Fehlen aktiver Maßnahmen und die Existenz von Kontrollgremien.

bar auf politische Gegner im In- und Ausland Einfluss nehmen.[11] Inwiefern die Informationsbeschaffung unter Einsatz heimlicher Methoden erfolgen muss, wird unterschiedlich beantwortet.[12]

Daneben findet sich der Begriff des Nachrichtendienstes.[13] Die Befugnisse eines Nachrichtendienstes reichen in der Regel weniger weit als die eines Geheimdienstes. Die nachrichtendienstliche Arbeit beschränkt sich im Wesentlichen auf das Sammeln, Auswerten und Weiterleiten von Informationen an exekutive Entscheidungsträger.[14] Im Gegensatz zu den Geheimdiensten bleibt den Nachrichtendiensten die aktive politische Einflussnahme verwehrt.[15] Diese Behördenform wird zum Teil als Nachrichtendienst im engeren Sinne bezeichnet.[16] Die zwischen Nachrichtendiensten im engeren und im weiteren Sinne differenzierende Ansicht setzt Nachrichtendienste im weiteren Sinne mit dem Begriff des Geheimdienstes gleich.[17]

In der Umgangssprache werden die Termini der Geheim- und Nachrichtendienste oftmals synonym verwendet.[18] In rechtlicher Hinsicht sollten mit dem Ende des Zweiten Weltkrieges Geheimdienste im klassischen Sinne abgeschafft und durch ein Nachrichtendienstwesen ersetzt werden. Dieser Systemwandel beruht auf den Erfahrungen mit der nationalsozialistischen Willkürherrschaft, deren Polizei- und Geheimdienstwesen durch eine zunehmende Auflösung rechtsstaatlicher Garantien geprägt war. Durch die Übertragung der Polizeigewalt auf das Reich sowie die personale Verschmelzung polizeilicher und parteilicher Strukturen kam es zu einer schrittweisen Zentralisierung,[19] Politisierung[20] und Entstaatlichung des Sicherheits-

---

[11] Vgl. u.a. *Baier,* S. 5 Fn. 10; *Gröpl*, S. 35ff; *König,* S. 23ff; *Kornblum,* S. 30; *Rehbein,* S. 25ff; *Zöller,* Informationssysteme, S. 285. Entgegen der landläufigen Bekanntheit werden die Charakteristika eines Geheimdienstes weder im Grundgesetz noch auf einfacher Gesetzesebene ausdrücklich definiert. Allein die Strafnorm des § 99 StGB verweist auf die Strafbarkeit einer geheimdienstlichen Tätigkeit für eine fremde Macht. Der Gesetzeskommentierung können jedoch zumindest Hinweise zum inhaltlichen Verständnis entnommen werden.

[12] Nach *Rose-Stahl,* S. 18, ist eine besondere Heimlichkeit nicht zwingend erforderlich.

[13] Vgl. vertiefend *König,* S. 23; *Rehbein,* S. 24ff. Daneben findet sich zusätzlich der Begriff der Verfassungsschutzbehörden. Vgl. die Begriffsbestimmungen in Art. 73 I Nr. 10b GG; § 1 I BVerfSchG; *König,* S. 26ff; *Roewer,* § 1 BVerfSchG Rn. 5; *Rödder,* S. 3f; *Rose-Stahl,* S. 29. Danach obliegt den Verfassungsschutzbehörden der Schutz der freiheitlichen demokratischen Grundordnung, des Bestands und der Sicherheit des Bundes oder eines Landes. Neben den vorliegend relevanten, nachrichtendienstlichen Aspekten werden hiervon zusätzlich die Bereiche des strafrechtlichen und verfassungsgerichtlichen Verfassungsschutzes erfasst.

[14] Vgl. *Zöller,* Informationssysteme, S. 285.

[15] Zudem unterliegen sie einer viel strikteren rechtlichen Kontrolle, so *Albert,* in: Korte/Zoller, S. 88.

[16] So etwa *Roewer,* § 3 BVerfSchG Rn. 4.

[17] *König,* S. 23, *Rose-Stahl,* S. 17f, *Zöller,* Informationssysteme, S. 285, lehnen diese Unterscheidung als überholt ab.

[18] Vgl. *Rose-Stahl,* S. 17; *Singer,* OK, S. 10.

[19] Vgl. *König,* S. 56.

apparates.[21] Diese Konzeption führte zu einer systematischen Überwachung der Bevölkerung durch den Sicherheitsdienst (SD)[22] und die Geheime Staatspolizei (Gestapo), die ihrerseits intensiv zusammenarbeiteten. Während dem SD eine umfassende Informationserhebung gestattet war, konnte die Gestapo Einzelfälle weitgehend ohne gesetzliche Bindungen und unter Einsatz exekutiver Befugnisse verfolgen. Regimegegner wurden ohne gerichtliche Kontrolle überwacht, eingeschüchtert oder verhaftet.[23] Das in diesem System angelegte Missbrauchspotential versuchten die Besatzungsmächte nach Beendigung des Zweiten Weltkrieges aufzubrechen.[24] Der während der Besatzungszeit die Regierungsgewalt ausübende sogenannte Alliierte Kontrollrat ordnete die Beseitigung des politischen Polizeiwesens sowie die Auflösung zahlreicher Verbände und Organisationen an.[25] Hiervon waren unter anderem die Gestapo, der SD sowie die SA und SS betroffen.[26] Damit beendeten die Reformen der Nachkriegszeit sowohl die Existenz eines politischen Polizeiwesens als auch die Institution der Geheimdienste als solche. Die Abschaffung des Geheimdienstwesens führte jedoch nicht zu einem vollständigen Verzicht auf staatliche Überwachungsstrukturen. Bereits in den Jahren von 1946 bis 1956 wurde als Reaktion auf steigende Kriminalitätszahlen, wirtschaftliche Schwierigkeiten und den schwelenden Ost-West-Konflikt ein neues Behördensystem eingeführt.[27] Vorbedingung der Alliierten war allerdings der Verzicht auf polizeiliche Befugnisse.[28] Die neu geschaffenen und bis heute existierenden Überwachungsstrukturen wurden dementsprechend nicht als Geheim-, sondern als Nachrichtendienste konzipiert. Im deutschen Kontext ist damit die Bezeichnung der Dienste als Nachrichtendienste zutreffend.[29]

---

[20] So etwa zwischen der Kriminalpolizei und der SS der NSDAP, vgl. *König,* S. 56.

[21] Vgl. hierzu insgesamt *Boldt/Stolleis,* in: Lisken/Denninger/Rachor, S. 25; *König,* S. 56.

[22] Dabei handelt es sich um die nachrichtendienstliche Einrichtung der NSDAP; vgl. *Kornblum,* S. 37.

[23] Vgl. *Albert,* ZRP 1995, S. 106; *König,* S. 59f; *Nehm,* NJW 2004, S. 3291; *Zöller,* JZ 2007, S. 763ff.

[24] Vgl. *König,* S. 63ff.

[25] Vgl. hierzu *Kornblum,* S. 37; *Thamm,* in: Hirschmann/Leggemann, S. 236.

[26] Vgl. hierzu *Imle,* S. 25ff, sowie *König,* S. 63; *Thamm,* in: Hirschmann/Leggemann, S. 236.

[27] Vgl. *König,* S. 67; *Thamm,* in: Hirschmann/Leggemann, S. 236. Insgesamt zu den Entwicklungen von 1949 bis 1968 vgl. *Boldt/Stolleis,* in: Lisken/Denninger/Rachor, S. 30ff. Insbesondere die im Zuge des Kalten Krieges auftretenden militärischen Spannungen zwischen der Sowjetunion und den Vereinigten Staaten gaben den Anstoß für die Errichtung der „Organisation Gehlen“ im Jahre 1946, dem Vorläufer des heutigen BND. Die Vorgänger des BfV und des MAD wurden erst im Jahr 1950 bzw. 1956 errichtet.

[28] Das insofern relevante Trennungsgebot wird unter Teil 2, III.A. näher dargelegt.

[29] So auch *Rehbein,* S. 26.

2. USA

Im amerikanischen Recht stehen die Begriffe der *intelligence* beziehungsweise des *intelligence services* im Mittelpunkt. Grundlage der im englischsprachigen Raum zur Anwendung kommenden *intelligence*-Definitionen ist in der Regel die Abgrenzung vom Begriff der *information*. Beide Begriffe stehen zueinander in einer Art Stufenverhältnis, beginnend mit *information* auf der untersten Stufe und *intelligence* auf der obersten Stufe. Die Abgrenzung erfolgt danach, wie umfassend das Ausgangsmaterial auf seine Aussagekraft und Verlässlichkeit hin untersucht wurde.[30] Der Begriff der *information* erfasst unbearbeitete Daten über Personen, Ereignisse oder Vorgänge, die noch keinem Bewertungs- oder Analyseprozess unterzogen wurden und damit nur geringfügig Schlussfolgerungen zulassen.[31] Die unbearbeitete *information* steht folglich am Anfang dieses Analyseprozesses, dessen Endprodukt *intelligence* ist. *Intelligence* wird daher zum Teil auch als *information with value-added analysis* verstanden (vgl. Abb. 1).[32] Der Prozess der Informationsverarbeitung wird als *intelligence cycle* bezeichnet.[33] Dieses Verständnis wird von manchen durch ein organisationsbezogenes Element ergänzt. Danach erfasst der Begriff *intelligence* Informationen, die von bestimmten Behörden in einem proaktiven Umfeld erhoben wurden.[34] Pro-aktives Handeln bezeichnet dabei üblicherweise Ermittlungen im Vorfeld begangener Straftaten.[35]

Abgesehen von diesem Grundverständnis kann der Begriff *intelligence* seinerseits in verschiedene, nicht immer einheitliche Unterkategorien aufgesplittet werden. Ein erster Kategorisierungsversuch unterscheidet die verschiedenen *intelligence*-Kategorien nach dem Zweck der Analyse. Diese Herangehensweise führt zu einer Aufteilung in *law enforcement intelligence* beziehungsweise *criminal intelligence* einerseits und *national security intelligence* andererseits. Die *law enforcement intelligence* soll die Strafverfolgungsbehörden bei der Aufklärung und Verhinderung von Straftaten in taktischer und strategischer Hinsicht unterstützen.[36] Demgegenüber dient *national security intelligence* dem Erhalt der Vereinigten Staaten als freier Staat und dem Schutz seiner verfassungsrechtlichen Grundlagen gegen Bedrohungen.[37] Andere Autoren differenzieren nach dem geografischen Bezugspunkt. Sie unterscheiden nach *foreign intelligence*, *domestic intelligence* und

---

30 Vgl. *Masse,* CRS 2006, S. 2.

31 Vgl. *Carter,* S. 9.

32 So etwa *Walker*, S. 2.

33 Vgl. *M. Albrecht,* in: Borchert, S. 47.

34 So etwa *Vervaele,* RIDP/IRPL 2009, S. 111.

35 Vgl. *Kühne*, Strafprozessrecht, S. 1281.

36 Vgl. hierzu *Carter*, S. 11.

37 Vgl. *Carter*, S. 14. Der Begriff der *national security intelligence* unterteilt sich seinerseits in *policy intelligence* und *military intelligence*.

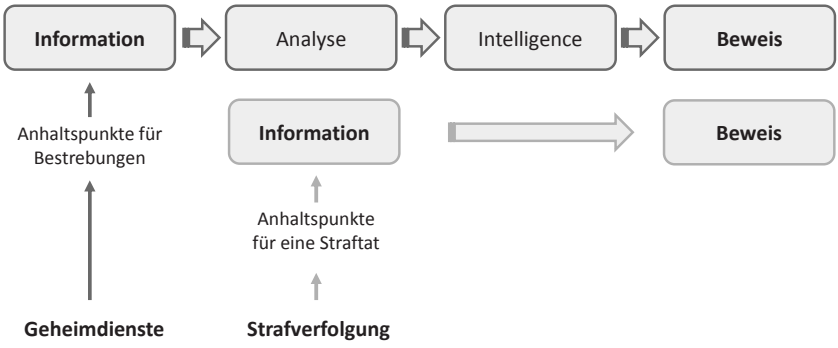

Abbildung 1: Weg von der Information zum Beweismittel

military intelligence mit *homeland security intelligence* als gemeinsamen Überschneidungsbereich.[38] Gemeinsames Element bleibt die nationale beziehungsweise innere Sicherheit, wobei der Ursprung der Bedrohung bei *foreign intelligence* im Ausland, bei *domestic intelligence* im Inland und bei *military intelligence* im militärischen Bereich liegt. *Homeland security intelligence* erfasst demgegenüber die innere Sicherheit im Allgemeinen, unabhängig davon, woher die Bedrohung kommt.

Im Bereich der nationalen Sicherheit unterscheidet der amerikanische Gesetzgeber ebenfalls zwischen unterschiedlichen Arten von *intelligence*.[39] Maßgeblich ist dabei die Aufteilung in *foreign intelligence* und *counterintelligence*.[40] Der Begriff der *foreign intelligence* beschreibt im Schwerpunkt Informationen, die sich auf Fähigkeiten, Absichten oder Aktivitäten ausländischer Regierungen, Organisationen oder internationale Aktivitäten des Terrorismus beziehen.[41] Erfasst werden zudem Informationen, die unter anderem gebraucht werden, um die Vereinigten Staaten gegen feindliche Attacken ausländischer Mächte oder ihrer Agenten, Sabotage, den internationalen Terrorismus und Waffenhandel zu schützen oder die nationale Verteidigung zu gewährleisten.[42] Der Begriff *counterintelligence* erfasst

---

[38] Vgl. *Masse,* CRS 2006, S. 5.

[39] Vgl. die 50 U.S.C. § 401a (1) *(intelligence)*, (3) *(counterintelligence)*, § 1801(e) *(foreign intelligence information)*.

[40] 50 U.S.C. § 401a (2), (3). In 50 U.S.C. § 401a (5) wird zusätzlich auf *national intelligence* als allgemeinen Oberbegriff verwiesen.

[41] Nach 50 U.S.C. § 401a (2) beschreibt der Begriff *foreign intelligence:* “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities”.

[42] Nach 50 U.S.C. § 1801(e): “‘foreign intelligence information’ means information that […] is necessary to […] protect against […] actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage, international terrorism, or

demgegenüber die Sammlung von Informationen und die Vornahme von Maßnahmen zum Schutz vor Spionage, geheimdienstlichen Tätigkeiten, Sabotage oder Attentaten, die durch oder zugunsten einer ausländischen oder internationalen Gruppierung begangen wurden.[43]

Eine zusätzliche Abgrenzung nach dem Bezugsobjekt der Überwachungsmaßnahmen ist auf die Rechtsprechung des *Supreme Court* zurückzuführen. Danach sind neben den bereits beschriebenen *foreign intelligence investigations* (FII) zusätzlich die *domestic (security) intelligence investigations* (DII) von Relevanz. Der Bereich der FII umfasst insofern nachrichtendienstliche Tätigkeiten in Bezug auf Bedrohungen und Spionagetätigkeit ausländischer Mächte oder deren Agenten, während es sich bei DII um Ermittlungen zum Schutz vor inländischen Bedrohungen ohne Auslandsbezug handelt.[44] Beide sammeln Erkenntnisse, die zum Schutz des Bestands und der Sicherheit der Nation erforderlich sind und sich daher von rein strafrechtlichen Ermittlungen abgrenzen.[45] Allerdings unterliegen Erkenntnisse der *domestic security intelligence* (DI) aufgrund der Involvierung von US-Bürgern weit strikteren Bindungen als Erkenntnisse der *foreign intelligence* (FI) mit Auslandsbezug beziehungsweise ausländischen Zielobjekten. Die Unterscheidung von FII und DII ist für die Untersuchung im amerikanischen Landesbericht von zentraler Bedeutung.

3. Zwischenergebnis

Dieser Überblick gibt einen ersten Eindruck der im deutschen und amerikanischen Geheimdienstrecht vorzufindenden sprachlichen Vielfalt. Sowohl der Begriff *intelligence* mit seinen zahlreichen Unterkategorien als auch die Bezeichnungen „Geheimdienst“ und „Nachrichtendienst“ sind durch sprachliche und historische Besonderheiten der nationalen Rechtsordnungen geprägt. Diese Unterschiede erschweren eine Zuordnung der relevanten Untersuchungsgegenstände. Zwar wird

---

the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power […] the national defense or the security of the United States […]”.

[43] Nach 50 U.S.C. § 401a (3) beschreibt der Begriff *counterintelligence:* “information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities”.

[44] Siehe hierzu den sog. *Keith* case – *United States v. United States District Court*, 407 U.S. 297, 322 (S. Ct. 1972). Zu dieser Unterscheidung vgl. *Chiarella/Newton,* Army Law, 1997, S. 27f. Als Beispiel für einen Fall der DII wird der Bombenanschlag in Oklahoma City angeführt, bei dem keine Verbindung zu einer ausländischen Macht oder einer internationalen Organisation nachgewiesen werden konnte.

[45] *United States v. United States District Court*, 407 U.S. 297, 322 (S. Ct. 1972) in Bezug auf DII “domestic security surveillance may involve different policy and practical considerations from the surveillance of ‘ordinary crime’”.

der Begriff des *intelligence service* oftmals vereinfacht mit Geheim- oder Nachrichtendienst übersetzt.[46] Die unterschiedlichen Begriffsmerkmale haben jedoch verdeutlicht, dass diese Institutionen gerade nicht deckungsgleich sind. Letztlich findet sich kein gemeinsamer Oberbegriff, der unproblematisch in beiden Rechtsordnungen angewendet werden könnte.

B. Terminologische Präzisierung

Um den Bedürfnissen des funktionalen Rechtsvergleichs gerecht zu werden, muss dem Begriff der Geheimdienstinformation eine konkrete Definition zugrunde gelegt werden. Die nachfolgenden Fragen präziseren die relevanten und typischen Kernelemente des als Geheimdienstinformation bezeichneten Wissens.

– *Wer erhebt Geheimdienstinformationen?*

  Die Untersuchung fokussiert sich auf die Informationsgewinnung durch staatliche Einrichtungen oder Behördeneinheiten. Dieses Merkmal dient der Abgrenzung zu privaten Nachrichtenagenturen, Politikberatungen oder *think tanks*.

– *Was ist inhaltlicher Gegenstand der Informationsbeschaffung?*

  Die Informationsbeschaffung konzentriert sich auf außen- und innenpolitische Bedrohungslagen. Diese müssen unter anderem die innere und äußere Sicherheit, den Bestand und die verfassungsrechtlichen Grundlagen des Staates und damit überragend wichtige Rechtsgüter gefährden. Hiervon werden etwa politisch motivierte Gewalttaten und Spionagetätigkeiten erfasst. Ein konkreter Tat- oder Täterbezug ist nicht erforderlich. Das überwachte Verhalten muss dementsprechend weder gesetzeswidrig noch strafrechtlich relevant sein. Die Informationsgewinnung ist primär zukunftsbezogen. Dieses Merkmal unterscheidet sie von Ermittlungen, die von vorneherein auf eine strafrechtliche Aburteilung zielen.

– *Wofür werden diese Informationen benötigt?*

  Die Informationen sollen primär den exekutiven Entscheidungsträgern die Einschätzung aktueller oder künftiger Risiken erleichtern. Sie werden daher im Anschluss an die Erhebung einer Auswertung unterzogen.

– *Wie werden die Informationen erhoben?*

  Die Informationen werden frühzeitig, langfristig und umfassend erhoben. Aufgrund der überragend wichtigen Rechtsgüter dürfen die zuständigen Dienste weitreichende, oftmals geheime Ermittlungsmethoden einsetzen. Geheimdienstinformationen zeichnen sich durch ein hohes Maß an Informationstiefe und -breite aus. Dieses Merkmal dient zur Abgrenzung von den klassischen Beweiserhebungsregeln.

---

[46] Beispielsweise *Romain/Byrd/Thielecke,* S. 584.

Das durch diese Behörden produzierte Wissen wird im untechnischen Sinn als Geheimdienstinformation, nachrichtendienstliche Erkenntnis oder als *intelligence* bezeichnet. Die beschriebenen Merkmale sind nicht abschließend zu verstehen. Aufgrund der historischen und nationalen Besonderheiten können die verschiedenen Elemente in der jeweiligen Rechtsordnung vielmehr unterschiedlich stark ausgeprägt sein. Die genannten Aspekte bilden lediglich den Ausgangspunkt des funktionalen Rechtsvergleichs. In Anlehnung daran werden in den Landesberichten diejenigen Behörden herausgestellt, die dieser Definition am nächsten kommen und die wesentlichen Kernmerkmale erfüllen. Der Schwerpunkt der Untersuchung wird auf die Informationserhebung im Inland gelegt.

Teil 2

Nutzung von Geheimdienstinformationen im deutschen Strafprozess

Die Nutzung von Geheimdienstinformationen im Strafprozess wird zunächst für den deutschen Landesbericht dargelegt. Die Darstellung gliedert sich in vier Teile. Im ersten Teil werden die für die Problematik relevanten Grundlagen des deutschen Strafverfahrensrechts herausgearbeitet (I.). Im zweiten Teil werden die Behörden dargestellt, die bei funktionaler Betrachtung Geheimdienstinformationen i.S.d. beschriebenen Definition produzieren (II.). Im dritten Teil werden geheimdienstliche Ermittlungen in die deutsche Sicherheitsarchitektur eingeordnet und deren Auswirkung auf die Informationsnutzung untersucht (III.). In einem vierten und abschließenden Teil werden die Auswirkungen nationaler Sicherheitsinteressen auf die Nutzung und Offenlegung von Geheimdienstinformationen behandelt (IV.).

I. Relevante Grundlagen des deutschen Strafprozessrechts

Die beweisrechtliche Nutzung von Geheimdienstinformationen muss die Vorgaben des allgemeinen Verfahrensrechts beachten. Dies erfordert eine kurze Einführung in relevante Grundsätze des deutschen Beweis- und Strafverfahrensrecht. Es werden die zentralen Rechtsquellen und die Gestaltung des deutschen Strafverfahrens (A.), die allgemeinen Grundprinzipien und Grenzen des deutschen Beweisrechts (B.) sowie die Zuständigkeiten bei geheimdienstrelevanten Strafsachen behandelt (C.). Die Darstellung konzentriert sich auf die für die Arbeit wichtigen Aspekte.

A. Rechtsquellen und Verfahrensablauf

Die wichtigste Quelle des deutschen Strafverfahrensrechts ist die Strafprozessordnung.[1] Daneben sind die Vorgaben des GVG, der RiStBV[2] sowie die Verbürgungen der EMRK von Bedeutung.[3] Diese Vorgaben werden durch die Ausle-

---

[1] Vgl. *Roxin/Schünemann,* § 1 Rn. 1, § 3 Rn. 1ff.

[2] Hierbei handelt es sich um eine allgemeine dienstliche Anweisung i.S.d. § 146 GVG.

[3] Vgl. insgesamt *Roxin/Schünemann,* § 3 Rn. 1ff.

gungsempfehlungen der Strafprozesslehre ergänzt.[4] Als „angewandtes Verfassungsrecht“[5] muss es zudem mit den verfassungsrechtlichen Normen und den Grundrechten in Einklang stehen.[6] Die Grundsätze der Beweisführung werden daher maßgeblich durch die Strafprozessordnung, das Verfassungsrecht sowie die Anmerkungen der Wissenschaft geprägt.

Das deutsche Strafverfahren gliedert sich in Ermittlungs-, Zwischen- und Hauptverfahren.[7] Ein Ermittlungsverfahren wird mit Vorliegen eines Anfangsverdachts i.S.d. § 152 II StPO eingeleitet.[8] In diesem werden die für das Hauptverfahren erforderlichen Beweise durch die Staatsanwaltschaft, den Ermittlungsrichter oder die Polizei erhoben. Der mutmaßliche Täter wird in diesem Verfahrensabschnitt als Beschuldigter bezeichnet. Es wird geprüft, ob ein genügender Anlass zur Erhebung einer öffentlichen Klage vorliegt. Besteht ein hinreichender Tatverdacht, erhebt die Staatsanwaltschaft die öffentliche Klage gemäß § 170 I StPO. Der Beschuldigte wird hierdurch zum Angeschuldigten gemäß § 157 StPO. Nach Anklageerhebung legt die Staatsanwaltschaft die zusammengestellten Akten dem zuständigen Gericht vor. Dieses prüft im sogenannten Zwischenverfahren, ob ein hinreichender Tatverdacht besteht und ob das Hauptverfahren zu eröffnen ist.[9] Das Gericht klärt, ob der Angeschuldigte der Straftat hinreichend verdächtig ist und damit aufgrund der vorläufigen Beweislage eine Aburteilung wahrscheinlich erscheint.[10] Fällt auch diese Entscheidung positiv aus, wird das Hauptverfahren eröffnet. Mit dem Eröffnungsbeschluss wird der Betroffene als Angeklagter bezeichnet. In der sich anschließenden Hauptverhandlung erfolgt die endgültige Beweisaufnahme beziehungsweise Tatsachenfeststellung.[11] Lediglich die in diesem Verfahrensabschnitt vorgetragenen Umstände dürfen dem Urteil zugrunde gelegt werden.[12] In der Rechtswirklichkeit wird die Hauptverhandlung jedoch maßgeblich durch die Ergebnisse des Ermittlungsverfahrens vorgeprägt. Defizite im Ermittlungsverfahren sind häufig nicht mehr korrigierbar und setzen sich im Rahmen des Hauptverfahrens fort.[13]

---

[4] Vgl. *Meyer-Goßner*, Einl. Rn. 5.

[5] Vgl. hierzu BVerfG NJW 1964, S. 1139, 1142f; BVerfG NJW 1972, S. 1123, 1125.

[6] So *Meyer-Goßner*, Einl. Rn. 5. Es handelt sich folglich gerade nicht um einen Parteiprozess.

[7] Davor findet wiederum das sog. staatsanwaltschaftliche Vorermittlungsverfahren statt, vgl. KK-*Pfeiffer/Hannich,* Einl. Rn. 34. Die Teilung des Strafverfahrens geht auf die RStPO von 1877 zurück, vgl. *Großkopf,* S. 20. Vertiefend *Roxin/Schünemann,* § 4 Rn. 1ff.

[8] Vgl. zum Ermittlungs- bzw. Vorverfahren §§ 151–177 StPO.

[9] Vgl. zum Zwischenverfahren §§ 199–211 StPO.

[10] Vgl. *Meyer-Goßner*, § 203 Rn. 2.

[11] Vgl. *Gleß,* S. 54, 58.

[12] Vgl. *Gleß,* S. 57; *Kühne,* Strafprozessrecht, Rn. 714; *Roxin/Schünemann,* § 4 Rn. 1.

[13] So *Kramer,* Rn. 169. Zur Hauptverhandlung als bloße Bestätigung der bereits im Ermittlungsverfahren erzielten Erkenntnisse vgl. *Peters,* S. 195.

B. Grundprinzipien und Grenzen der Beweisführung

Das deutsche Beweisrecht wird von zwei wesentlichen Grundprinzipen beherrscht. Diese betreffen die Pflicht zur Wahrheitserforschung aus § 155 II, § 244 II StPO sowie den Grundsatz der freien Beweiswürdigung nach § 261 StPO.[14] Diese Vorgaben stellen die Person des Richters in den Mittelpunkt.

Um der Pflicht zur Wahrheitserforschung zu genügen, muss der Richter die Beweisaufnahme von Amts wegen auf alle entscheidungserheblichen Tatsachen und Beweismittel erstrecken.[15] Der Sachverhalt ist vollständig und unter Heranziehung der sachnächsten beziehungsweise bestmöglichen Beweise auszuforschen.[16] Hierdurch sollen die materielle Wahrheit ermittelt, der staatliche Strafanspruch verwirklicht und das materielle Schuldprinzip durchgesetzt werden.[17] Diese Aufgabe nimmt der Richter selbstständig wahr, ohne an Anträge der Prozessbeteiligten gebunden zu sein. Über das Ergebnis dieser Beweisaufnahme entscheidet der Richter schließlich nach seiner freien, aus der Hauptverhandlung geschöpften Überzeugung. Bei der Würdigung der vorgetragenen Beweismittel ist der Richter grundsätzlich nicht an starre Beweisregeln gebunden.[18] Seine Entscheidung muss allerdings auf einer ausreichend tragfähigen Tatsachengrundlage beruhen, den Anforderungen der Logik genügen und darf gesicherten wissenschaftlichen Erkenntnissen beziehungsweise allgemeinen Erfahrungssätzen nicht widersprechen.[19] Zu dieser Beweiswürdigung ist der Richter nur in der Lage, wenn sämtliche entscheidungserheblichen Tatsachen in der Hauptverhandlung mündlich und möglichst unvermittelt vorgetragen wurden.[20] Die Aufklärungspflicht und die freie Beweiswürdigung bauen dementsprechend unmittelbar aufeinander auf.[21] Können Zweifel auf Tatsachenebene trotz Ausschöpfung aller Beweismittel nicht hinreichend ausgeräumt werden, ist der Angeklagte freizusprechen.[22] Der Zweifelssatz gilt für Tatsachen, die für Fragen der Schuld oder der Strafbarkeit von unmittelbarer Bedeu-

---

[14] Vgl. hierzu insgesamt *Eisenberg,* Rn. 1; *Roxin/Schünemann,* § 45 Rn. 2ff, 42ff. Zum Verhältnis der Wahrheitserforschung und Beweiswürdigung vgl. *Trüg,* S. 203ff.

[15] BGH NJW 2007, S. 2269, 2271.

[16] Sog. materielles Unmittelbarkeitsprinzip; vgl. insgesamt *Eisenberg,* Rn. 11, 13.

[17] Zur Ermittlung des wahren Sachverhalts als zentrales Anliegen des Strafprozesses vgl. u.a. BVerfG NStZ 1987, S. 419; *Eisenberg,* Rn. 2; *Trüg,* S. 62.

[18] Vgl. KK-*Pfeiffer/Hannich,* Einl. Rn. 117. Das Prinzip der freien Beweiswürdigung wird damit als Abkehr von den starren Beweisregeln des Inquisitionsprozesses verstanden, vgl. Graf-*Eschelbach,* § 261 Rn. 1.

[19] Vgl. KK-*Schoreit,* § 261 Rn. 45ff.

[20] Sog. Mündlichkeitsprinzip und formelles Unmittelbarkeitsprinzip. Das Mündlichkeitsprinzip kommt in den §§ 250, 261, 264 StPO zum Ausdruck und bildet eine grundlegende Bedingung für den Anspruch auf rechtliches Gehört nach Art. 103 I GG und den Grundsatz der Öffentlichkeit nach § 169 GVG, Art. 6 I EMRK, vgl. *Eisenberg,* Rn. 11, 64.

[21] So *Eisenberg,* Rn. 2.

[22] Vgl. *Eisenberg,* Rn. 116, 120.

tung sind.[23] Die Anwendung dieses Grundsatzes steht damit im engen Zusammenhang zum Rechtsstaatsprinzip, dem Schuldprinzip und der Unschuldsvermutung.[24] Der Zweifelssatz bildet eine Entscheidungsregel für den Fall, dass der Richter zu keiner Überzeugung gelangen kann.[25] Er kommt folglich erst nach Abschluss der Beweiswürdigung zur Anwendung.

Die Pflicht zur Wahrheitserforschung und das Gebot zur umfassenden Beweiswürdigung gelten nicht bedingungslos.[26] Sie können vielmehr durch das Vorliegen eines Beweisverbotes beschränkt werden.[27] Beweisverbote unterteilen sich in sogenannte Beweis*erhebungs*verbote und Beweis*verwertungs*verbote.[28] Erstere schränken die Möglichkeiten der Strafverfolgungsbehörden bei der Beweiserhebung ein. Bestimmte Themen werden von der Wahrheitserforschung ausgeschlossen, bestimmte Mittel oder Methoden dürfen nicht angewandt werden. Beweisverwertungsverbote begrenzen dagegen den sich anschließenden Verwertungsprozess. Danach dürfen bestimmte Erkenntnisse oder Sachverhalte in der gerichtlichen Beweiswürdigung nicht berücksichtigt werden.[29]

Verwertungsverbote lassen sich in drei verschiedene Kategorien untergliedern. In der ersten Kategorie wird die Unverwertbarkeit bereits im ausdrücklichen Gesetzeswortlaut angeordnet.[30] Diese Gruppe ist aufgrund der eindeutigen gesetzlichen Fixierung weitgehend unproblematisch. Die zweite Kategorie leitet sich aus einem Verstoß gegen eine Beweiserhebungsvorschrift ab. In diesem Fall spricht man von einem sogenannten unselbstständigen Beweisverwertungsverbot.[31] In der dritten Kategorie resultiert das Verwertungsverbot aus der Verfassung beziehungsweise den Grundrechten selbst.[32] Da ein vorgelagerter Verstoß gegen eine Beweiserhe-

---

[23] Vgl. *Roxin/Schünemann,* § 45 Rn. 59.

[24] Vgl. insgesamt *Roxin/Schünemann,* § 45 Rn. 56ff.

[25] Vgl. *Eisenberg,* Rn. 118. Der Zweifelssatz bildet damit gerade keine Leitlinie zur Würdigung der Beweise i.S. einer Beweis(last)regel, vgl. KK-*Schoreit,* § 261 Rn. 56.

[26] Die Wertungen des Grundgesetzes gestatten keine Wahrheitserforschung „um jeden Preis", vgl. u.a. BGH in BGH NJW 1960, S. 1580, 1582. Insbesondere unter Verweis auf das Rechtsstaatsprinzip des Art. 20 III GG. Erstmals wohl bei *von Beling,* S. 17, so auch *Roxin/Schünemann,* § 24 Rn. 22; vgl. zudem *Trüg,* S. 64; *Rehbein,* S. 139.

[27] Vgl. *Roxin/Schünemann,* § 45 Rn. 54. Allerdings können Verwertungsverbote auch in umgekehrter Richtung zur Wahrheitsfindung beitragen, wie dies bei den §§ 250ff StPO der Fall ist. Vgl. zu diesem Spannungsverhältnis *Amelung,* NJW 1991, S. 2534.

[28] Vertiefend bei Vgl. *Roxin/Schünemann,* § 24 Rn. 15ff.

[29] Vgl. BGHSt 31, 304, 308; *Pfeiffer* StPO*,* § 261 Rn. 117.

[30] Beispiele hierfür sind etwa die §§ 138a III 2, 100a IV 2 StPO; vgl. *Roxin/Schünemann,* § 24 Rn. 22.

[31] Zur Unterscheidung zwischen selbstständigen und unselbstständigen Beweisverwertungsverboten vgl. stellvertretend *Beulke,* Rn. 457ff. Diese Unterscheidung ablehnend *Roxin/Schünemann,* § 24, dort unter Fn. 2.

[32] Vertiefend bei *Meyer-Goßner*, Einl. Rn. 56ff.

bungsvorschrift nicht erforderlich ist, spricht man in diesem Fall von einem selbstständigen Verwertungsverbot. Anders als bei den unselbstständigen Verwertungsverboten sind diese bei einer rechtmäßigen Beweiserhebung denkbar. Wann in der zweiten und dritten Kategorie von einem Verwertungsverbot auszugehen ist, bestimmt sich nach einer Abwägung im Einzelfall.[33] In dieser wird das Interesse an der Strafverfolgung dem Interesse des Bürgers an der Wahrung seiner Rechte gegenübergestellt. Relevante Abwägungskriterien sind die Schwere des konkret zu verfolgenden Delikts, das Gewicht des Verfahrensverstoßes, die Bedeutung des betroffenen Rechtsguts sowie der Schutzzweck der verletzten Norm.[34] Die Abwägungsfähigkeit im konkreten Einzelfall bestimmt sich nach der sogenannten Sphärentheorie. Diese Theorie unterscheidet mit Intim-, Privat- und Sozialsphäre drei verschiedene Bereiche. Der Eingriff in die Intimsphäre führt immer zu einem Beweisverwertungsverbot. Sie betrifft den absoluten, abwägungsresistenten Kernbereich privater Lebensgestaltung.[35] Eingriffe in den kernbereichsfremden Teil der Privatsphäre sind demgegenüber einer Einzelfallabwägung zugänglich und können durch überwiegende Allgemeininteressen gerechtfertigt werden. Eingriffe in den äußeren Kreis – die Sozialsphäre sind in beweisrechtlicher Hinsicht grundsätzlich unbeachtlich. Beweisverwertungsverbote folgen damit insgesamt keinem Automatismus, sondern resultieren aus einer Abwägung der verschiedenen gegenläufigen Interessen. Faktisch handelt es sich dabei um eine Art Verhältnismäßigkeitsprüfung. Die Grenzen der Beweisführung basieren damit im Wesentlichen auf materiellen beziehungsweise individualschutzrechtlichen Erwägungen.[36]

In der Praxis bilden Beweisverwertungsverbote eine begründungsbedürftige Ausnahme.[37] Angesichts eines rechtsstaatlichen Bedürfnisses an einer funktionstüchtigen Strafrechtspflege darf das Interesse an der Wahrheitsfindung nur bei übergeordneten wichtigen Gründen im Einzelfall zurückgestellt werden.[38] Das Prinzip der freien Beweiswürdigung führt schließlich dazu, dass im Grundsatz

---

[33] Vgl. BGH NJW 2007, S. 2269, 2271; BGH NJW 1999, S. 959, 961, unter Verweis auf die gefestigte Rechtsprechung. Vgl. zu den verschiedenen Ansätzen, wie etwa der früher vom BGH vertretenen Rechtskreistheorie sowie der sich daran anlehnenden Schutzzwecklehre u.a. *Eisenberg,* Rn. 365f; *Grünwald,* JZ 1966, S. 489; *Pelz,* S. 108ff; *Rehbein,* S. 149ff; *Roxin/Schünemann,* § 24 Rn. 23ff sowie BGHSt 46, 189, 195 zu § 252 StPO. Diese Theorien sind oftmals nicht in der Lage, einen allgemeingültigen Begründungsansatz zu liefern. Vgl. zur Diskussion *Pelz,* S. 108ff; *Rehbein,* S. 149ff; *Amelung,* NJW 1991, S. 2534ff.

[34] Vgl. u.a. BGH NJW 2007, S. 2269, 2271.

[35] Vgl. *Kühne,* FS für Roxin, Rn. 1285.

[36] Vgl. *Herrmann,* FS für Jescheck, S. 1293; *Rehbein,* S. 155. Die Mehrheit der Beweisverbote leiten sich dabei aus den Persönlichkeitsrechten und der Privatsphäre ab, sei es in Bezug auf die Willensfreiheit, den Schutz der Intimsphäre oder der Familie.

[37] BVerfG NJW 2010, S. 2937, 2938; BGH HRRS 2009 Nr. 890, Rn. 47, sowie *Adam,* NStZ 2010, S. 325.

[38] Vgl. u.a. BGH HRRS 2009 Nr. 890, Rn. 47; BGHSt 37, 30, 32; *Joecks*, Einl. Rn. 188ff.

zunächst jedes Beweismittel zuzulassen ist. Der Richter entscheidet dann als Korrektiv über deren Beweiskraft.[39] Kommt er zur Annahme eines Beweisverwertungsverbots, darf das Beweismittel nicht in die Beweiswürdigung und damit nicht in die Entscheidungsfindung einbezogen werden.[40] Wurde ein unverwertbares Beweismittel in die Hauptverhandlung eingeführt, muss der Richter dieses Wissen daher ausblenden. Ein solches Verwertungsverbot wird der Richter vor allem bei schwerwiegenden Verstößen, wie beispielsweise einer bewussten oder willkürlichen Umgehung einer Verfahrensvorschrift, annehmen.[41]

Die Wirkung eines Beweisverwertungsverbots ist im Grundsatz auf die unmittelbare Beweisnutzung begrenzt.[42] Die weit überwiegende Meinung lehnt eine pauschale Fernwirkung von Beweisverboten ab.[43] Vor dem Hintergrund der Inquisitionsmaxime und des Legalitätsprinzips soll ein einziger Verfahrensverstoß nicht das gesamte Strafverfahren „lahmlegen" dürfen, da dies das Vertrauen der Bürger in eine funktionstüchtige Rechtspflege beeinträchtigen könnte.[44] Dieses Verständnis führt dazu, dass ein Verwertungsverbot in den meisten Fällen lediglich die Verwertung des unmittelbar betroffenen Beweismittels beschränkt und sich nur im Ausnahmefall zusätzlich auf die mittelbar erhaltenen Erkenntnisse erstreckt. Die Fernwirkung ist entsprechend des Regel-Ausnahme-Verhältnisses als solche begründungsbedürftig. Wann ein solcher Ausnahmefall vorliegt, richtet sich nach der konkreten Sachlage sowie nach Art und Schwere des Verstoßes.[45] Als bereits anerkannte Ausnahmefälle gelten die bewusste Missachtung von Verfahrensvorschriften oder besonders schwerwiegende Verstöße.[46] Daneben wurde vom BGH aufgrund des massiven Eingriffs in Art. 10 GG eine Fernwirkung für § 7 III G10 a.F. angenommen.[47]

In verfahrensrechtlicher Hinsicht ist ein Verwertungsverbot als Ausfluss des Ermittlungsgrundsatzes im Grundsatz von Amts wegen zu berücksichtigen.[48] Zum Teil macht die Rechtsprechung die Wirkung des Verwertungsverbots allerdings

---

[39] Vgl. *Amelung,* NJW 1991, S. 2534.

[40] Vgl. *Eisenberg,* Rn. 356.

[41] Vgl. BGH NJW 2007, S. 2269, 2272 m.w.N. Ebenso in Bezug auf die fehlerhafte Durchsuchung *Meyer-Goßner*, § 98 Rn. 7. Zur Umgehung des Richtervorbehalts und die daran anzuknüpfenden Folgen vgl. ausführlich *Brüning,* HRRS 2007, S. 250ff.

[42] Vgl. *Rehbein,* S. 141; *Roxin/Schünemann,* § 25 Rn. 64.

[43] Stellvertretend für viele *Meyer-Goßner*, § 136a Rn. 31. Zum Streitstand vgl. u.a. BGH NJW 1980, S. 1700f, sowie *Weichert,* S. 222f. A.A. *Spendel,* NJW 1966, S. 1108.

[44] Vertiefend *Roxin/Schünemann,* § 25 Rn. 59.

[45] BGH NJW 1980, S. 1700f.

[46] Vgl. *Kramer,* Rn. 792; *Roxin/Schünemann,* § 25 Rn. 59f.

[47] Vgl. BGH NJW 1980, S. 1700, *Lohberger,* FS für Hanack, S. 262; *Roxin/Schünemann,* § 25 Rn. 59.

[48] Vgl. *Herrmann,* FS für Jescheck, S. 1306; *Trüg,* S. 476.

von einem fristgerechten und begründeten Widerspruch des Angeklagten beziehungsweise seines Verteidigers abhängig.[49] Diese Obliegenheit besteht indes nur, wenn dem Angeklagten ein Verteidiger zur Seite steht oder er zuvor vom Gericht über die Notwendigkeit eines Widerspruchs belehrt wurde. Verzichtet er auf die Einlegung des Widerspruchs, wird der frühere Eingriff nachträglich geheilt. Diese Widerspruchslösung wurde ursprünglich für den Bereich der Belehrungspflichten entwickelt. In jüngster Zeit hat die Rechtsprechung allerdings den Anwendungsbereich der Widerspruchslösung erweitert, sodass deren konkrete Reichweite nicht eindeutig feststeht. Die ergänzten Fallgruppen betreffen vor allem unselbstständige Beweisverwertungsverbote, die auf einer der Verletzung subjektiver prozessualer Rechte beruhen.[50] Wird in diesem Sinne die Anwendbarkeit der Widerspruchslösung bejaht, entsteht das richterliche Beweisverwertungsverbot erst nach Einlegung des Widerspruchs.

C. Zuständigkeiten bei geheimdienstrelevanten Straftaten

Die Nutzung von Geheimdienstinformationen kommt vor allem bei Delikten im Bereich des Staatsschutzes in Betracht.[51] Grundsätzlich werden Strafverfolgung und Strafgerichtsbarkeit den Staatsanwaltschaften und Gerichten der Bundesländer zugewiesen, Art. 30 und 92 GG.[52] Von dieser Grundregel gestattet Art. 96 V Nr. 5 GG eine Ausnahme. Demnach kann der Bundesgesetzgeber im Bereich der Staatsschutzstrafsachen die Ausübung der Bundesgerichtsbarkeit durch die Gerichte der Länder gesetzlich festlegen und diese im Wege der Organleihe einbinden.[53]

Die konkrete Zuordnung eines Delikts zum Bereich des Staatsschutzes und damit zur Bundesjustiz wird nach Art. 74 I Nr. 1 GG dem Bundesgesetzgeber überlassen. Dieser kann die Zuständigkeit allerdings nicht beliebig erweitern. Er kann die Ausnahmezuständigkeit nur bei Delikten begründen, die einen länderübergreifenden Charakter aufweisen oder Rechtsgüter des Gesamtstaates in einer Weise beeinträchtigen, welche das Eingreifen der Bundesjustiz erforderlich machen.[54] Eine

---

[49] Vgl. insgesamt zur Widerspruchslösung *Kuhn,* JA 2010, S. 891ff. Diese ablehnend *Bertram,* S. 272; *Rogall,* JZ 2008, S. 830; *Roxin/Schünemann,* § 24 Rn. 34.

[50] Vgl. Löwe/Rosenberg-*Schäfer,* § 110d Rn. 40.

[51] Vertiefend zum Begriff des Staatsschutzes *T. Wollweber,* S. 88ff, 102ff.

[52] Vgl. KK-*Hannich,* § 120 GVG Rn. 1a.

[53] Vgl. *Backhaus*, S. 21ff; Graf-*Huber,* § 120 GVG Rn. 2; KK-*Hannich,* § 120 GVG Rn. 3; Maunz/Dürig-*Jachmann,* Art. 96 Rn. 56f; *Nehm*, Zuständigkeit, S. 11; *T. Wollweber*, S. 149ff; *Welp*, NStZ 2002, S. 3, 5.

[54] Vgl. BGH NJW 2002, S. 1889; BGH NStZ 2001, S. 265, 268; KK-*Hannich,* § 120 GVG Rn. 1a; *Nehm*, Zuständigkeit, S. 12.

solche Regelung hat der Gesetzgeber mit § 120 I, II GVG getroffen. Diese überträgt in bestimmten Fällen die erstinstanzliche Zuständigkeit auf die Oberlandesgerichte der jeweiligen Landeshauptstadt.[55] Diese Zuständigkeitskonzentration soll eine gewisse Sachkunde des urteilenden Richters sicherstellen. Im Übrigen verbleibt es bei der Regelzuständigkeit der Länder.[56]

Die Zuständigkeit der Oberlandesgerichte kann nach § 120 I, II GVG als unbedingte oder bedingte Zuständigkeit begründet werden.[57] Eine unbedingte Zuständigkeit besteht beim Vorliegen einer der in §§ 120 I, 142a I GVG genannten Straftaten.[58] Der Katalog des § 120 I GVG ist abschließend und umfasst vor allem die klassischen Staatsschutzdelikte.[59] Als taugliche Begehungsformen werden sowohl Täter-, als auch Teilnahme- und Vorbereitungshandlungen erfasst.[60] Eine bedingte Zuständigkeit nach §§ 120 II, 142a I GVG besteht, wenn der Generalbundesanwalt in den gesetzlich vorgesehenen Fällen durch die Ausübung seines Evokationsrechts Anklage beim OLG erhebt.[61] In dieser Funktion übt der Generalbundesanwalt als oberste Strafverfolgungsbehörde des Bundes das Amt der Staatsanwaltschaft aus.[62] Trotz seiner organisatorischen Zuordnung als politischer Beamter der Exekutive agiert er als notwendiges Organ der Strafrechtspflege und ist damit in funktionaler Hinsicht der Judikative zuzuordnen.[63]

Das Bestehen einer beweglichen Zuständigkeit bestimmt sich nach den Varianten des § 120 II Nr. 1–4 GVG. Nach § 120 II Nr. 1 GVG wird die Zuständigkeit bei Vorliegen von einem der in § 74a I GVG genannten Staatsschutzdelikte begründet. Für eine Zuständigkeit nach § 120 II Nr. 2 GVG bedarf es einer bestimmten schweren Straftat, die im Zusammenhang mit einer ausländischen terroristischen Vereinigung steht. Bezugspunkt sind damit ausländische Vereinigungen mit selbstständigen Teilorganisationen in Deutschland, deren Zweck oder Tätigkeit die Begehung von Straftaten wie Mord, Totschlag oder einer der in § 129 a I Nr. 2, II StGB genannten Straftaten zum Gegenstand hat.[64] Für eine Zuständigkeit nach § 120 II

---

[55] Vgl. Graf-*Huber,* § 120 GVG Rn. 1; KK-*Hannich,* § 120 GVG Rn. 2.

[56] Zur Beachtung des Regel-/Ausnahmeverhältnisses *Nehm*, Zuständigkeit*,* S. 13.

[57] Vertiefend *T. Wollweber,* S. 155ff, 176ff.

[58] Vgl. *Backhaus*, S. 22f; Graf-*Huber,* § 120 GVG Rn. 2.

[59] Vgl. *Eisenberg*, NStZ 1996, S. 264.

[60] Vgl. KK-*Hannich*, § 120 GVG Rn. 3.

[61] Vgl. Graf-*Huber,* § 120 GVG Rn. 3f.

[62] Ausführliche Informationen finden sich auf der offiziellen Internetseite des Generalbundesanwalts unter www.generalbundesanwalt.de/de/straf.php [Stand: 1.5.2012]. Vertiefend *T. Wollweber,* S. 28ff.

[63] Siehe zu dieser Bezeichnung § 54 I Nr. 5 Bundesbeamtengesetz. Vgl. zur Stellung des Generalbundesanwalts den offiziellen Auftritt unter www.generalbundesanwalt.de/de/stellung.php [Stand: 1.5.2012].

[64] Vgl. *Backhaus,* S. 24.

Nr. 3 GVG bedarf es einer bestimmten schweren Straftat, die nach den Umständen bestimmt und geeignet ist, den Bestand oder die Sicherheit des Staates zu beeinträchtigen oder die Verfassungsgrundsätze der Bundesrepublik Deutschland zu beseitigen, außer Geltung zu setzen oder zu untergraben. Es genügt die konkrete Eignung der Tat, welche der Täter gekannt und in seinen Willen aufgenommen haben muss.[65] Durch diese Variante werden grundsätzlich individualschützende Straftatbestände der Allgemeinkriminalität der Bundeskompetenz unterstellt, sofern im Einzelfall eine staatsgefährdende Relevanz vorliegt.[66] In § 120 II Nr. 4 GVG wird schließlich in bestimmten Fällen eine Zuständigkeit für Straftaten nach dem Außenwirtschafts- und Kriegswaffenkontrollgesetz begründet.

In allen vier Varianten des § 120 II GVG ist zusätzlich erforderlich, dass der Generalbundesanwalt wegen der besonderen Bedeutung des Falls die Verfolgung übernimmt. Dieses Merkmal orientiert sich nicht an den klassischen strafrechtlichen Kriterien, sondern versteht sich als Bedeutsamkeit im staatsschutzrechtlichen Sinne.[67] Es soll als einschränkendes Moment verhindern, dass politische Straftaten allein aufgrund ihrer Zielsetzung der Länderzuständigkeit entzogen werden. Die Annahme einer besonderen Bedeutung des Falls erfordert demnach ein staatsgefährdendes Delikt von erheblichem Gewicht, das den Gesamtstaat in einer derart spezifischen Weise angreift, dass ein Einschreiten des Generalbundesanwalts geboten ist.[68] Neben der Korrektivwirkung soll dieses Merkmal dem Staat eine von starren Straftatkatalogen losgelöste und damit flexible Handhabung des dynamischen Staatsschutzbegriffs ermöglichen.[69] In diesem Sinne wurde unter anderem durch die Einfügung des § 120 II 1 Nr. 3 GVG die ursprünglich auf Organisationsdelikte beschränkte Verfolgungskompetenz des Generalbundesanwalts auf Staatsschutzdelikte von Einzeltätern erweitert.[70]

---

[65] Vgl. *Nehm*, Zuständigkeit, S. 18. Eine Absicht ist nicht erforderlich; vgl. BGH NStZ 2001, S. 265, 269.

[66] Vgl. *Backhaus,* S. 24.

[67] Vgl. *Nehm*, Zuständigkeit, S. 22.

[68] Vgl. BGH NStZ 2008, S. 146, 2. Leitsatz; BGH NStZ 2009, S. 335, 338; BGH NStZ 2002, S. 447f; BGH NJW 2001, S. 1359, 1363; *Diemer*, NStZ 2005, S. 667; *Welp*, NStZ 2002, S. 7; *T. Wollweber,* S. 215ff. Beispiele bei KK-*Hannich,* § 120 GVG Rn. 3; *Nehm*, Zuständigkeit, S. 23f.

[69] Vgl. *Nehm*, Zuständigkeit, S. 15. Ähnlich *T. Wollweber,* S. 177f.

[70] Vgl. Gesetz zur Bekämpfung des Terrorismus vom 19.12.1986, BGBl. I, 1986, S. 2566. Siehe zum Entstehungsgrund der Norm *T. Wollweber,* S. 195f.

II. Produzenten von Geheimdienstinformationen

A. Die klassischen deutschen Dienste

In der deutschen Sicherheitsarchitektur sind die Nachrichtendienste die klassischen Produzenten von Geheimdienstinformationen. Das deutsche Nachrichtendienstwesen umfasst namentlich das Bundesamt für Verfassungsschutz (BfV) inklusive der 16 Landesämter, das Amt für den Militärischen Abschirmdienst (MAD) sowie den Bundesnachrichtendienst (BND).[117] Abgrenzungsmerkmal ist der jeweils abweichende (territoriale) Einsatzschwerpunkt. In dieser Hinsicht wurde dem Verfassungsschutz die Inlandsaufklärung, dem BND die Auslandsaufklärung und dem MAD die Aufklärung innerhalb der Streitkräfte übertragen.

1. Die Inlandsaufklärung, insbesondere BfV

Die Inlandsaufklärung wird in Deutschland durch das Bundesamt für Verfassungsschutz (BfV) und 16 weitere Landesbehörden wahrgenommen. Auf Landesebene ist der Verfassungsschutz entweder in eigenständigen Landesämtern für Verfassungsschutz oder als Abteilung eines Landesinnenministeriums organisiert.[118]

Die Zuständigkeitsabgrenzung erfolgt nach § 5 BVerfSchG. Danach wird die operative Arbeit überwiegend durch die Landesbehörden wahrgenommen, welche ihre Erkenntnisse an das BfV übermitteln.[119] Dem BfV obliegt in diesem Zusammenhang als Zentralstelle primär die Koordination der Landesämter. Im Verhältnis zu den Landesbehörden besteht jedoch weder ein Über-Unterordnungsverhältnis noch ein Weisungsrecht. Die Beteiligten sind entsprechend der Zusammenarbeitspflicht nach § 1 II BVerfSchG vielmehr allgemein zu einer kooperativen Zusammenarbeit verpflichtet.[120] Das BfV als Bundesbehörde ist lediglich zuständig, wenn ein bundesweiter Bezug vorliegt, auswärtige Belange berührt oder mehrere Bundesländer involviert sind.[121] Organisatorisch ist das BfV nach § 2 I 2 BVerfSchG

---

[117] Diesen wird durch Gesetz der Status eines Nachrichtendienstes zugesprochen.

[118] LfV existieren in Baden-Württemberg, Bayern, Bremen, Hamburg, Hessen, Niedersachsen, dem Saarland und Thüringen. In Berlin, Brandenburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt und Schleswig-Holstein wird die Arbeit durch eine Abteilung des Landesinnenministeriums vorgenommen; vgl. hierzu *Rehbein,* S. 28.

[119] Vgl *Rehbein,* S. 28.

[120] Allein die Bundesregierung hat nach § 7 BVerfSchG ein Weisungsrecht, nicht jedoch das BfV; vgl. *Baier,* S. 6; *Rose-Stahl,* S. 40.

[121] Vgl. § 5 II BVerfSchG. Daneben kann es auf Ersuchen eines Landesamtes für Verfassungsschutz tätig werden; vgl. *Daun,* in: Jäger/Daun, S. 64.

dem Innenministerium zugeordnet.[122] Dieses übt über das BfV die Rechts-, Fach- und Dienstaufsicht aus.

Die Gesetzgebungs- und Einrichtungskompetenz des Bundes für das BfV findet sich in Art. 73 Nr. 10 b, c, 87 I 2 GG, auf deren Grundlage das Bundesverfassungsschutzgesetz (BVerfSchG) erlassen wurde.[123] Auf Landesebene können die Landesgesetzgeber nach Art. 30, 70 I GG die Aufgaben und Befugnisse ihrer jeweiligen Landesämter für Verfassungsschutz frei bestimmen, sofern sie nicht in den Kompetenzbereich des Bundes eingreifen oder durch eine Verengung der Befugnisse die notwendige Zusammenarbeit gefährden.[124] Die Befugnisse der Landesverfassungsschutzbehörden sind daher weitgehend parallel oder sogar umfassender formuliert als diejenigen des BfV. Da eine umfassende Darstellung sämtlicher länderspezifischen Besonderheiten den Rahmen dieser Untersuchung sprengen würde, werden die im BVerfSchG enthaltenen Vorgaben der vorliegenden Untersuchung als eine Art Grundkonsens zugrunde gelegt.[125] Auf etwaige Besonderheiten wird bei Bedarf eingegangen.

Die Aufgaben des BfV bestimmen sich nach §§ 3, 4 BVerfSchG. Danach obliegt dem BfV rein formal zunächst die Sammlung und Auswertung von Informationen über bestimmte Bestrebungen oder Tätigkeiten.[126] Der Begriff des Sammelns erfasst sowohl die passive Entgegennahme als auch die aktive Beschaffung der vom Beobachtungsauftrag umfassten Erkenntnisse.[127] „Auswerten“ beschreibt die Aufarbeitung von Informationen, durch welche die einzelnen Wissenselemente zu einem Gesamtbild zusammengefügt und auf ihre Richtigkeit hin kontrolliert werden.[128] Das Merkmal der Bestrebung erfasst ziel- und zweckgerichtete, politisch bestimmte Verhaltensweisen in einem oder für einen Personenzusammenschluss.[129] Daneben kann sich der Beobachtungsauftrag auf Tätigkeiten beziehen. Der Begriff der Tätigkeit ist umfassender als derjenige der Bestrebung. Er erfasst jedes menschliche Tun. Eine subjektive Zielsetzung, wie im Falle der Bestrebungen, ist nicht erforderlich. Es genügen objektiv sicherheitsgefährdende beziehungsweise geheimdienstliche Verhaltensweisen.[130] Die beobachtbaren Bestrebungen oder Tätigkeiten

---

[122] Das BfV selbst unterteilt sich in 6 Abteilungen. Darunter befinden sich unter anderem eine Abteilung zum Islamismus und islamistischen Terrorismus (Abteilung 6).

[123] Vgl. zum BVerfSchG BGBl. I, 1990, S. 2954ff

[124] Vgl. *Droste,* Handbuch, S. 52; *Rehbein,* S. 28f.

[125] Vgl. zur Notwendigkeit einer solchen Begrenzung auch *Rehbein,* S. 29.

[126] Vgl. *Droste,* Handbuch, S. 87ff.

[127] Vgl. *Droste*, Handbuch, S. 87f.

[128] Vgl. bei *Rehbein,* S. 30; *Roewer,* S. 57. Vertiefend *Droste,* Handbuch, S. 89.

[129] Vgl. § 4 BVerfSchG sowie vertiefend *Droste,* Handbuch, S. 165ff; Borgs-Maciejewski/Ebert-*Borgs*, § 3 BVerfSchG Rn. 49ff; *Roewer,* § 3 BVerfSchG Rn. 15; *Schafranek,* S. 59ff; *Singer,* OK, S. 183ff, 187ff.

[130] Vgl. § 3 I Nr. 2 BVerfSchG.

können sich auf unterschiedliche Beobachtungsfelder beziehen.[131] Hierzu zählen unter anderem Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder auf eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes abzielen.[132] Hiervon werden schwerpunktmäßig Bestrebungen des politischen Extremismus und Terrorismus erfasst.[133] Weiterhin kann sich die Beobachtung auf Aspekte der Spionageabwehr oder des Ausländerextremismus erstrecken.[134] Mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 wurde schließlich der Beobachtungsauftrag auf völkerverständigungswidrige Bestrebungen erweitert.[135] Die Arbeitsfelder des BfV umfassen folglich vor allem die Bereiche des Extremismus, des Terrorismus, der Spionage- und Proliferationsabwehr sowie den Geheim-, Sabotage- und Wirtschaftsschutz.[136] Die Arbeit des Verfassungsschutzes bezieht sich damit insgesamt auf außen- und innenpolitische Bedrohungslagen.

Beobachtungsobjekt sind in der Regel keine Einzelpersonen, sondern Personenzusammenschlüsse. Der Gesetzgeber ging folglich davon aus, dass entsprechende Großgefahren üblicherweise von Personenmehrheiten drohen.[137] Ausreichend für eine Zuordnung zu dieser Personenmehrheit ist jedoch die Mitgliedschaft in einer entsprechenden terroristischen beziehungsweise extremistischen Vereinigung.[138] Verhaltensweisen von sonstigen Einzelpersonen werden nur dann erfasst, wenn diese zusätzlich die Voraussetzungen des § 4 I 4 BVerfSchG erfüllen. Danach ist eine gewisse Ernsthaftigkeit der Hilfestellung erforderlich.[139] Der Beobachtungsauftrag der Verfassungsschutzbehörden ist damit im Grundsatz organisationsbezogen.[140] Diese können ihn frühzeitig und ohne Bindung an das Legalitätsprinzip ausüben.

---

131 Vertiefend zu den materiellen Aufgaben und Gefahrtatbeständen vgl. *Droste,* Handbuch, S. 92ff; 175ff.

132 Vgl. zu diesen Voraussetzungen §§ 3 I Nr. 1, 4 BVerfSchG.

133 So *Zöller,* JZ 2007, S. 765.

134 Vgl. § 3 I Nr. 2, 3 BVerfSchG; *Droste,* Handbuch, S. 117; *Zöller,* JZ 2007, S. 765.

135 Vgl. § 3 I Nr. 4 BVerfSchG; BGBl. I, 2002, S. 361. Kritisch dazu *Roggan,* in: Roggan/Kutscha, S. 439f. Dieser bezweifelt die ausreichende Bestimmtheit der Norm sowie das Bestehen der erforderlichen Gesetzgebungskompetenz. Vertiefend zur Neuregelung *Baldus,* ZRP 2002, S. 400ff.

136 Da sich Aktivitäten des internationalen Terrorismus gegen die Grundordnung des demokratischen Rechtsstaates richten und sich hierbei extremistischer und friedensgefährdender Taktiken bedienen, kann dieser Bereich mehreren Beobachtungsfeldern zugeordnet werden; vgl. *Zöller,* JZ 2007, S. 765.

137 Vgl. *Singer,* OK, S. 184.

138 Hierdurch werden die Bestrebungen des Personenzusammenschlusses i.S.d. § 4 I 2 BVerfSchG nachdrücklich unterstützt; vgl. *Droste,* Handbuch, S. 173.

139 Vgl. *Droste,* Handbuch, S. 172f; *Singer,* OK, S. 184.

140 Trotz der Bezugnahme auf die Zielgerichtetheit der Verhaltensweise muss die handelnde Person noch nicht bekannt sein. So *Roewer,* § 3 BVerfSchG Rn. 18.

Die Informationserhebung durch den Verfassungsschutz erfolgt nach offiziellen Angaben zu einem überwiegenden Teil aus offen zugänglichen Quellen. Der Gesamtanteil dieser Form der Informationserhebung wird größtenteils auf einen Anteil von 60 % bis 80 % geschätzt.[141] Offen zugängliche Quellen sind etwa Zeitungsartikel, Internetbeiträge, Rundfunksendungen, Informationsmaterialien öffentlicher Veranstaltungen oder Massenmedien jeglicher Art. Der übrige Anteil von ca. 20 % entfällt demnach auf sogenannte nachrichtendienstliche Mittel. Nach § 8 II BVerfSchG erfasst dies beispielsweise heimliche Maßnahmen, wie den Einsatz von Vertrauensleuten[142] und Gewährspersonen, verdeckte Operationen, sowie Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen.[143] Diese prozentuale Verteilung wird zum Teil bestritten.[144] Die Kritiker verweisen darauf, dass dieses vermeintlich offen zugängliche Material häufig nur i.V.m. nachrichtendienstlichen Mitteln verfügbar ist. Druckerzeugnisse extremistischer Vereinigungen seien oftmals nur durch die Einschleusung von V-Leuten, das heißt angeworbenen Personen der extremistischen Szene, erhältlich. Zum Teil wird daher von einem Anteil von 40 % ausgegangen.[145] Auf der Grundlage dieser Erkenntnisse werden zudem die jährlich erscheinenden Verfassungsschutzberichte veröffentlicht. Diese sollen die Öffentlichkeit über die Arbeit des Verfassungsschutzes aufklären und über extremistische Gruppierungen informieren. Zudem stellt das BfV die Erkenntnisse dem Bundesinnenministerium zur Verfügung. Es versteht sich selbst als „Frühwarnsystem der Demokratie".[146]

Neben der Wahrnehmung des beschriebenen Beobachtungsauftrags ist der BfV nach § 3 II 1 BVerfSchG i.V.m. dem Sicherheitsüberprüfungsgesetz zusätzlich an Sicherheitsüberprüfungen beteiligt. Diese sollen gewährleisten, dass Schlüsselpositionen in staatlichen wie nichtstaatlichen Einrichtungen nicht von risikobehafteten Personen besetzt und sabotiert werden sowie sensible Informationen nicht nach

---

141 Vgl. *Droste,* Handbuch, S. 228; *Rose-Stahl,* S. 65. Inwiefern diese Prozentzahlen tatsächlich die praktische Relevanz widerspiegeln, ist unklar.

142 Unter V-Leuten werden Privatpersonen verstanden, die von einer Behörde zur Gewinnung von Informationen eingesetzt werden, ohne dieser organisatorisch anzugehören. Ihr Einsatz erfolgt in der Regel langfristig und unter Geheimhaltung ihrer wahren Identität. Stellvertretend für viele *Eisenberg,* Rn. 1034a; *Lisken,* ZRP 2003, S. 46.

143 Vgl. hierzu den Internetauftritt des BfV unter www.verfassungsschutz.de unter der Rubrik „Wir über uns", „Was wir tun", „Was genau macht der Verfassungsschutz" [Stand: 1.5.2012]. Ebenso *Albert,* in: Korte/Zoller, S. 96. In den jeweiligen Verfassungsschutzgesetzen der Länder findet sich zumeist eine ähnliche Auflistung. Abweichungen sind in der Regel auf politische Gründe zurückzuführen, vgl. *Rödder,* S. 92.

144 Vgl. u.a. *Albert,* in: Korte/Zoller, S. 97ff, und *Rose-Stahl,* S. 66. Zu den verschiedenen Prozentzahlen vgl. die Übersicht bei *Rehbein,* S. 37 Fn. 74.

145 Vgl. zu dieser Kritik vgl. *Albert,* in: Korte/Zoller, S. 97.

146 Vgl. zum Selbstverständnis als Frühwarnsystem Bundesamt für Verfassungsschutz, Was wir für Sie tun, S. 9.

außen gelangen. Erfasst werden der personelle Geheimnisschutz (Nr. 1), der Sabotageschutz (Nr. 2) sowie der materielle Geheimnisschutz (Nr. 3).[147]

Erkenntnisse der Verfassungsschutzbehörden erfüllen damit sämtliche Kriterien der eingangs gewählten Definition von Geheimdienstinformationen.

2. Die Auslandsaufklärung, insbesondere BND

Die Auslandsaufklärung wird in Deutschland vor allem durch den Bundesnachrichtendienst (BND) betrieben. Dieser geht historisch gesehen auf die Organisation Gehlen zurück. Leiter und Namensgeber war Reinhard Gehlen. Dieser konnte den USA als ehemaliger Leiter der nachrichtlichen Abteilung der Wehrmacht „Fremde Heere Ost" und damit als Experte für das russische Militär wichtige Informationen und Intelligence-Strukturen zur Verfügung stellen.[148] Trotz seines nationalsozialistischen Hintergrundes sollte er die Informationsbeschaffung weiterführen und in enger Zusammenarbeit mit dem amerikanischen Auslandsnachrichtendienst CIA wichtige Erkenntnisse über den sowjetischen Gegner liefern.[149] Die Organisation Gehlen arbeitete daher nach dem Zweiten Weltkrieg mit der amerikanischen CIA in Fragen der Ostaufklärung zusammen. Am 1. April 1956 wurde der BND durch Kabinettsbeschluss vom Bund übernommen und der Bundesregierung unterstellt.[150] Heutzutage ist der BND sowohl für die zivile als auch die militärische Auslandsaufklärung zuständig.[151]

Die Gesetzgebungs- und Einrichtungskompetenz des Bundes für den BND folgt aus Art. 73 I Nr.1 GG und Art. 87 III 1 GG. Die einfachgesetzliche Grundlage bildet das Bundesnachrichtendienstgesetz, kurz BNDG. Organisatorisch ist der BND nach § 1 I 1 BNDG dem Geschäftsbereich des Bundeskanzleramts zugeordnet und unterrichtet nach § 12 BNDG das Bundeskanzleramt über seine Tätigkeit. Anders als das BfV ist er somit weder als Bundesoberbehörde i.S.d. Art. 87 III 1 1. Alt. GG noch als Zentralstelle i.S.d. Art. 87 I 2 GG konzipiert.[152]

---

147 Vgl. vertiefend *Rehbein,* S. 35; *Zöller,* JZ 2007, S. 765f.

148 Vgl. *Reese,* S. 19; *Daun,* in: Jäger/Höse/Oppermann, S. 173.

149 Vgl. *Kornblum,* S. 39; *Rose-Stahl,* S. 138.

150 Vgl. *Daun,* in: Jäger/Höse/Oppermann, S. 173; *Kornblum,* S. 39; *Reese,* S. 23; *Rieger,* ZRP 1985, S. 3; *Rose-Stahl,* S. 138.

151 Bei besonderen Auslandsverwendungen der Bundeswehr oder humanitären Maßnahmen kann allerdings auch der MAD im Ausland Aufgaben wahrnehmen, vgl. www.mad.bundeswehr.de sowie § 14 MADG. Zu den Tätigkeiten des MAD im Ausland *Brissa,* DöV 2011, S. 393.

152 Der BND untergliedert sich in zwölf Abteilungen. Darunter fallen u.a. die sog. technische Aufklärung (Abteilung TA) und die Abteilung Terrorismus (Abteilung TE).

Der Aufgabenbereich des BND erstreckt sich nach § 1 II BNDG allgemein auf die Beschaffung und Auswertung von „Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind". Erforderlich ist damit ein hinreichender Bezug zu auswärtigen Angelegenheiten i.S.d. Art. 73 I Nr. 1 GG sowie die Relevanz für Belange der äußeren Sicherheit.[153] Hiervon werden außenpolitische, wirtschaftliche, rüstungstechnische sowie Aspekte des internationalen Terrorismus und der internationalen organisierten Kriminalität erfasst.[154] Die grundsätzlich auslandsbezogene Informationserhebung kann allerdings auch im Inland erfolgen.[155] Einzelne Tätigkeitsfelder werden durch ein geheimes Auftrags- und Interessensprofil der Bundesregierung präzisiert.[156] Die Informationserhebung des BND erfolgt regelmäßig losgelöst von einem konkreten Verdacht oder Ereignis.[157] Seinen Aufklärungsauftrag erfüllt der BND unter Einsatz signalerfassender Quellen (SIGINT, insbesondere COMINT[158]) sowie der operativen Nutzung menschlicher Quellen (HUMINT[159]). Er nutzt damit insgesamt weitreichende und zum Teil geheime Methoden. Der BND versteht sich ebenfalls als Frühwarnsystem und Ansprechpartner für die Erstellung aussagekräftiger Risikoeinschätzungen.[160] Diese Funktion erfordert eine umfassende Informationserhebung. Das Vorliegen strafrechtlich relevanten Verhaltens ist nicht notwendig. Der BND erfüllt damit ebenfalls sämtliche Definitionsmerkmale eines Geheimdienstes und ist als tauglicher Produzent von Geheimdienstinformationen anzusehen.

---

153 Vgl. *Singer,* OK, S. 258.

154 Vgl. hierzu die Webseite des BND unter www.bnd.de unter dem Punkt „Struktur"; vgl. zudem *Daun,* in: Jäger/Daun, S. 61; *Pfeiffer,* ZRP 1994, S. 254; *Rieger,* ZRP 1985, S. 4; *Rose-Stahl,* S. 142; *Wolff,* S. 91.

155 Vgl. www.bnd.de sowie *Rose-Stahl,* S. 142; *Singer,* in: Jäger/Daun, S. 269. Die Zulässigkeit einer Inlandstätigkeit wird im Wortlaut des § 1 II BNDG deutlich. Darin geht es um besondere Voraussetzungen für Informationen, die „im Geltungsbereich dieses Gesetzes", also der Bundesrepublik Deutschland, erhoben wurden. In diesem Fall setzt § 1 II 2 BNDG der Informationserhebung besondere Grenzen; vgl. auch *Graulich,* in: Graulich/Simon, S. 155.

156 Vgl. *Daun,* in: Jäger/Daun, S. 61; *Graulich,* in: Graulich/Simon, S. 155; *Soiné,* DöV 2006, S. 204; *Rose-Stahl,* S. 141.

157 So etwa im Bereich der strategischen Überwachung nach dem G10-Gesetz.

158 SIGINT *(Signals Intelligence)* beschreibt die signalerfassende Aufklärung wie z.B. das Abfangen von Funk- oder anderen elektronischen Signalen wie Radar, Radio, Morse und sonstiger Datenübertragung. COMINT *(Communications Intelligence)* ist eine Unterkategorie von SIGINT und beschränkt sich auf die Fernmeldeaufklärung, d.h. die Überwachung von Kommunikationsmedien, wie Telefon, Email, Fax, Satellit und Radiowellen; vgl. u.a. *M. Albrecht,* in: Borchert, S. 49; *Daun,* in: Jäger/Höse/Oppermann, S. 175f.

159 HUMINT steht für *Human Source Intelligence* und erfasst die Informationsgewinnung durch den Einsatz menschlicher Quellen, wie Agenten; vgl. u.a. *M. Albrecht,* in: Borchert, S. 49; *Daun,* in: Jäger/Höse/Oppermann, S. 175f. Der BND ist der einzige deutsche Auslandsnachrichtendienst, der diese Beschaffungsmethode einsetzt.

160 Vgl. *Droste,* Nachrichtendienste, S. 101.

3. Die militärische Aufklärung

Die militärische Aufklärung erfolgt in Deutschland unter der Leitung des militärischen Nachrichtenwesens der Bundeswehr (MilNWBw). Dieses setzt sich aus dem Amt für den Militärischen Abschirmdienst (MAD) und dem Kommando Strategische Aufklärung (KSA) zusammen.[161]

a) Militärischer Abschirmdienst

Der dritte offizielle Nachrichtendienst auf Bundesebene ist der Militärische Abschirmdienst (MAD). Er ist innerhalb der Streitkräfte für die Extremismus- und Spionageabwehr zuständig und dient der Sicherung der Einsatzbereitschaft der Bundeswehr. Der MAD ging 1956 aus der Unterabteilung „Innere Sicherheit der Streitkräfte" des früheren Amt Blank hervor, das die Vorgängerbehörde des heutigen Bundesverteidigungsministeriums war und nach dem früheren Leiter *Theodor Blank* benannt wurde.[162] Die besagte Unterabteilung wurde bereits 1957 in „Amt für Sicherheit der Bundeswehr" und im Zuge der Umstrukturierung 1984 in „Amt für den Militärischen Abschirmdienst" umbenannt.[163]

Die verfassungsrechtlichen Grundlagen des MAD finden sich in den Art. 73 I Nr. 1, 10 b, 87a I 1 GG. Einfachgesetzlich werden die Aufgaben und Befugnisse in dem Gesetz über den militärischen Abschirmdienst, kurz MADG, festgelegt. Organisatorisch ist der MAD dem Bundesverteidigungsministerium zuzuordnen.[164] Er unterrichtet die Bundeswehrführung im Rahmen der ihm übertragenen Aufgaben.[165] Anders als das BfV ist er jedoch keine verwaltungsrechtlich selbstständige Bundesbehörde, sondern Teil der Streitkräfte.[166]

Der MAD nimmt die Aufgaben des Verfassungsschutzes im Geschäftsbereich des Verteidigungsministeriums wahr. Ihm sind damit diejenigen Angelegenheiten übertragen, die außerhalb der Streitkräfte durch das BfV wahrgenommen werden.[167] Diese Parallelität wird zum Teil durch den Verweis des MADG auf die

---

[161] Vgl. vertiefend zum MAD und dem MilNWBw *Brissa,* DöV 2011, S. 391ff. Das Zentrum für Nachrichtenwesen der Bundeswehr (ZNBw) wurde 2007 abgeschafft.

[162] Vgl. *Kornblum,* S. 42.

[163] Vgl. www.mad.bundeswehr.de; vgl. dort unter „Geschichte des Militärischen Abschirmdienstes", [Stand: 1.5.2012].

[164] Der MAD besitzt 5 Abteilungen, darunter u.a. die Abteilung II für die Extremismus-/ Terrorismusabwehr.

[165] Vgl. *Graulich,* in: Graulich/Simon, S. 153.

[166] Vgl. *Baier,* S. 8; *Rose-Stahl,* S. 131. Dem MAD kommt dabei keine Zentralstellenfunktion zu, *Kornblum,* S. 51.

[167] Vgl. *Engelhart,* in: Wade/Maljević, S. 513; *Singer,* in: Jäger/Daun, S. 269; *Wolff,* S. 91. Der MAD wird zum Teil als „Verfassungsschutz der Bundeswehr" bezeichnet, vgl. Innenministerium des Landes Nordrhein-Westfalen, S. 6.

Normen des BVerfSchG deutlich. Die wesentlichen Arbeitsbereiche erstrecken sich in Anlehnung an das BfV daher auf die Spionage-, Extremismus- und Terrorismusabwehr innerhalb der Bundeswehr.[168] Seit 2004 wurden dem MAD zusätzliche Aufgaben im Ausland übertragen.[169]

Der MAD erfüllt ebenfalls die wesentlichen Anforderungen der vorliegenden Geheimdienstdefinition.

b) Kommando Strategische Aufklärung

Das MilNWBw umfasst weiterhin das Kommando Strategische Aufklärung (KSA).[170] Dieses wurde im Jahr 2002 aufgrund der steigenden militärischen Aktivitäten Deutschlands errichtet. Anders als der MAD kann das KSA nicht auf eine einfachgesetzliche Grundlage zurückgreifen, sondern gründet sich allein auf Art. 87a GG.[171] Dem KSA ist zusammen mit dem BND die signalerfassende Aufklärung (SIGINT) im Ausland übertragen.[172] Daneben ist es zur Gewinnung von Bildmaterial mittels Satelliten, sogenanntem IMINT, befugt.[173] Die Informationserhebung des KSA ist thematisch auf militärisch relevante Bedrohungslagen begrenzt.[174] Das KSA nimmt damit vor allem militärisch relevante Geheimdienstfunktionen wahr. Obwohl das KSA offiziell vom Gesetz nicht als Nachrichtendienst eingestuft wird, produziert es ebenfalls Geheimdienstinformationen i.S.d. gewählten Definition.

---

168 Nach § 14 I MADG ist er auf Anordnung des Bundesministers zusätzlich befugt, Informationen zu erheben, die „zur Sicherung der Einsatzbereitschaft“ bzw. „zum Schutz der Angehörigen, der Dienststellen und Einrichtungen des Geschäftsbereichs des Bundesministeriums der Verteidigung erforderlich sind“; vgl. http://www.mad.bundeswehr.de [Stand: 1.5.2012] sowie *Rose-Stahl,* S. 137f.

169 Davor wurde die Auslandsaufklärung allein vom BND wahrgenommen, vgl. *Singer,* in: Jäger/Daun, S. 269.

170 Daneben existieren zudem die *Intelligence*-Abteilungen der Streitkräfte, vgl. *Daun,* in: Jäger/Höse/Oppermann, S. 172.

171 Zum Fehlen gesetzlicher Grundlagen und dem dadurch erforderlichen Rückgriff auf Verfassungsrecht vgl. *Brissa,* DöV 2011, S. 393. Dort findet sich auch der Verweis auf die „Zentrale Dienstvorschrift 2/1 – Das Militärische Nachrichtenwesen“ vom 28.10.2004, in der unter anderem Organisation, Auftrag und Aufgaben festgelegt werden, die jedoch als Verschlusssache der Geheimhaltung unterliegt.

172 Vgl. *Daun,* in: Jäger/Daun, S. 63.

173 IMINT steht für *Imagery Intelligence*; vgl. u.a. *Daun,* in: Jäger/Daun, S. 64. Diese Befugnis steht dem BND nicht zu.

174 Im Vergleich dazu kann der BND eine umfassende Auslandsaufklärung betreiben; vgl. *Daun,* in: Jäger/Daun, S. 64.

B. Mögliche Produzenten von Geheimdienstinformationen

Neben den klassischen Diensten existieren weitere Sicherheitsbehörden, die im Laufe der vergangenen Jahre beziehungsweise Jahrzehnte mit nachrichtendienstlichen Befugnissen ausgestattet wurden. Diese Einrichtungen könnten unter Umständen ebenfalls als Produzenten von Geheimdienstinformationen eingestuft werden. In Betracht kommen unter anderem das Zollkriminalamt (ZKA) und das Bundeskriminalamt (BKA).[175] Ergänzend wird zudem auf das Gemeinsame Terrorismusabwehrzentrum (GTAZ), das Gemeinsame Internetzentrum (GIZ) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingegangen.

1. Bundeskriminalamt

Das BKA unterstützt als überörtliche Behörde die Strafverfolgung im Inland.[176] Es wurde „zur Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten" geschaffen.[177] Angesichts dieses Aufgabenspektrums erscheint die Subsumtion unter die Geheimdienstdefinition zunächst falsch. Diese Einschätzung ist seit der Reform des BKAG durch das „Gesetz zur Abwehr von Gefahren des internationalen Terrorismus" in ihrer Pauschalität allerdings nicht mehr zutreffend.[178] Die maßgeblichen Änderungen traten mit Wirkung zum 1.1.2009 in Kraft und übertrugen dem BKA in § 4a i.V.m. §§ 20a–20x BKAG die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus.[179] Die damit verbundenen Befugnisse greifen anders als bisherige Ermächtigungen in einem operativen Vorfeldbereich, der dem traditionellen Gefahrbegriff vorgelagert ist.[180] Die Aufklärung in diesem Stadium soll bereits der Entstehung einer Gefahrenlage sowie der Begehung noch unbekannter, in ferner Zukunft liegender Straftaten entgegenwirken.[181] Das BKA besitzt damit erstmals präventive Befugnisse zur

---

[175] Vgl. § 1 I BKAG. Zur Zuordnung zum deutschen Geheimdienstwesen vgl. u.a. *Daun,* in: Jäger/Höse/Oppermann, S. 172. Ablehnend demgegenüber *Rehbein,* S. 86f.

[176] Vgl. *Forkert-Hosser,* S. 35.

[177] Dem BKA kommt hierbei eine Zentral-, Ermittlungs-, Schutz,- Verwaltungs- und internationale Funktion zu; vgl. vertiefend die Informationsbroschüre des BKA, abrufbar unter www.bka.de/profil/broschueren/profil2008.pdf [letzter Abruf 2.3.2011; hiernach BKA-Broschüre], sowie *Kretschmer,* JURA 2006, S. 337.

[178] Vgl. BGBl. Nr. 66 vom 31.12.2008, S. 3083.

[179] Eingehend *Harnisch/Pohlmann,* NVwZ 2009, S. 1328. Das BKA wird u.a. zur Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten mittels technischer Mittel, sog. IMSI-Catcher ermächtigt.

[180] Dies zeigt sich beim Vergleich des IMSI-Catchers, für dessen Einsatz die Ermittlungsschwelle in § 20n I i.V.m. § 20l I Nr. 2 BKAG gegenüber § 100i StPO deutlich abgesenkt ist; vgl. *Baum/Schantz,* ZRP 2008, S. 140.

[181] Vgl. *Harnisch/Pohlmann,* NVwZ 2009, S. 1329; *Roggan,* NJW 2009, S. 257. Kritisch zur „operativen Polizeiarbeit" vgl. *Denninger,* in: Lisken/Denninger/Rachor, S. 376ff.

Terrorismusbekämpfung.[182] Diese Vorfeldkompetenz i.V.m. einer umfassenden Erhebungsbefugnis erfasst Bereiche, die klassischerweise den Nachrichtendiensten zugewiesen waren und erfüllt damit zugleich wesentliche Merkmale der Geheimdienstdefinition.[183] Diese Änderungen waren unter anderem der Grund dafür, dass im Reformprozess zur Fortentwicklung der parlamentarischen Kontrolle vom 24.3.2009 eine Einbeziehung des BKA in die Kontrollmechanismen des Bundes diskutiert wurde.[184] Allerdings ist diese quasi-geheimdienstliche Befugnis des BKA auf wenige Anwendungsfälle begrenzt. Der Gesamtcharakter des BKA als kriminalpolizeiliche Behörde ändert sich dadurch nicht. Somit stellt das BKA zwar keinen Nachrichtendienst im klassischen Sinne dar, allerdings kann er zumindest in Teilbereichen als Produzent von Geheimdienstinformationen eingestuft werden.[185]

2. Zollkriminalamt

Daneben wird eine Zuordnung des Zollkriminalamts (ZKA) zum Geheimdienstsektor diskutiert.[186] Das ZKA fungiert gemäß §§ 2, 3 ZFdG unter anderem als Zentralstelle. In dieser Funktion unterstützt es beispielsweise die Arbeit der Zollverwaltung (§ 3 V ZFdG) und koordiniert die Arbeit der Zollfahndungsämter (§ 3 V ZFdG). Organisatorisch sind das ZKA und die Zollfahndungsämter dem Zollfahndungsdienst zuzuordnen.[187] Die Zollfahndung selbst gehört nach § 1 I ZFdG dem Bundesministerium der Finanzen an.

Neben der Koordinierungsfunktion sind dem ZKA nach § 4 ZFdG eigenständige Überwachungs- und Strafverfolgungsaufgaben zugewiesen, die sich thematisch auf Belange des Außenwirtschaftsverkehrs (Abs. 2), des grenzüberschreitenden Warenverkehrs (Abs. 3) und der organisierten Kriminalität im Bereich der Geldwäsche (Abs. 4) beziehen. In seiner Strafverfolgungsfunktion agiert das ZKA als Kriminalpolizei im Zuständigkeitsbereich der Zollverwaltung.[188] In seiner Überwachungsfunktion ist dem ZKA zudem die „Aufdeckung unbekannter Straftaten" über-

---

[182] Vgl. *Baum/Schantz,* ZRP 2008, S. 137; *Harnisch/Pohlmann,* NVwZ 2009, S. 1328.

[183] Zur Ähnlichkeit mit einem Geheimdienst vgl. u.a. *Roggan,* NJW 2009, S. 262; *Wolff,* JZ 2010, S. 173. Vgl. zur „Vernachrichtendienstlichung der Polizei" insgesamt *Wolff,* DöV 2009, S. 599 m.w.N., ebenso *Singer,* in: Jäger/Daun, S. 281.

[184] Vgl. zum ursprünglichen Gesetzesentwurf BT-Drs. 16/12411, S. 4. Danach sollten das BKA und das ZKA ebenfalls in die Kontrolle mit einbezogen werden. Dieser Passus wurde im Laufe des weiteren Gesetzgebungsverfahrens gestrichen, vgl. BT-Drs. 16/13220; *Huber,* NVwZ 2009, S. 1321f; *Wolff,* DöV 2009, S. 598.

[185] So jedenfalls *Singer,* in: Jäger/Daun, S. 281; *Rehbein,* S. 92f; *Ziercke,* in: Bundesamt für Verfassungsschutz, S. 48.

[186] Vgl. hierzu *Hamacher,* DStR 2006, S. 633ff, ablehnend *Rehbein,* S. 92f.

[187] Siehe § 1 I ZFdG.

[188] Zu diesem Zweck darf es u.a. auf die Ermächtigungen der StPO zurückgreifen.

tragen.[189] Diese Überwachungskompetenz knüpft weder an eine konkrete Gefahr i.S.d. Polizeirechts noch an einen Anfangsverdacht i.S.d. Strafprozessordnung an.[190] Ausreichend sind vielmehr „tatsächliche Anhaltspunkte" hinsichtlich geplanter Straftaten.[191] Das ZKA ist damit ebenfalls zu Vorfeldermittlungen befugt, die klassischerweise nur durch die Geheim- und Nachrichtendienste wahrgenommen werden.[192] Gleiches gilt für die angegliederten Zollfahndungsämter, denen nach § 26 II ZFdG für diesen Bereich sogar eine Eingriffsgeneralklausel zugestanden wurde.[193] Schließlich darf das ZKA besonders sensible Informationsbeschaffungsmethoden einsetzen, die bislang den traditionellen Nachrichtendiensten vorbehalten waren. Die §§ 20, 21 ZFdG gestatten dem ZKA beispielsweise die Datenerhebung durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes. Zur Unterbindung des Waffenhandels ist das ZKA nach § 23a ZFdG ferner zur Telekommunikationsüberwachung befugt. Diese Sonderstellung führte, ebenso wie beim BKA, zu einer Diskussion, ob das ZKA in die parlamentarische Kontrolle der nachrichtendienstlichen Tätigkeit des Bundes mit einbezogen werden sollte.[194] Der entsprechende Passus im Gesetzesentwurf wurde allerdings für beide Behörden im Laufe des weiteren Gesetzgebungsverfahrens gestrichen.[195] Die Art und Weise der Informationserhebung ist jedoch derjenigen der Geheim- und Nachrichtendienste stark angenähert, sodass die Zollfahndung zumindest in Teilbereichen in den Kreis der Produzenten von Geheimdienstinformationen einbezogen werden kann.

3. BSI, GTAZ und GIZ

Im Bereich der geheimdienstlichen Informationserhebung werden neben den bereits dargestellten Behörden oftmals die Einrichtungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Gemeinsamen Terrorismusabwehrzentrums (GTAZ) und des Gemeinsamen Internetzentrums (GIZ) genannt.

Die Abteilung 2 des BSI ist für die frühzeitige Informationserhebung und Schaffung von Lagebildern zuständig. Thematisch widmet sich das BSI der Entwicklung und Überprüfung sicherer Software und damit vor allem der IT-Sicherheit. Es ver-

---

189 Siehe §§ 4 II, III ZFdG.

190 Vgl. BT-Drs. 14/8007, S. 28; *Linke,* S. 190.

191 Vgl. BT-Drs. 14/8007, S. 28, unter Bezugnahme auf die Norm des § 208 I 1 Nr. 3 AO zur Aufdeckung unbekannter Steuerfälle.

192 Vgl. *Hirsch,* S. 34.

193 So *Linke,* S. 189ff.

194 So der Gesetzesentwurf die BT-Drs. 16/12411, S. 4.

195 Vgl. BT-Drs. 16/13220; *Huber,* NVwZ 2009, S. 1322, und *Wolff,* DöV 2009, S. 598. Allerdings finden sich auch Autoren, die eine Qualifizierung des ZKA als Geheimdienst ablehnen, wie beispielsweise *Hirsch,* S. 34.

steht sich als eine Art Dienstleister und Berater von Verwaltungsstellen, Herstellern und Nutzern von Informationstechnik.[196] Die Informationsgewinnung dient damit weder der Erhaltung der Handlungsfähigkeit einer Regierung, noch ist sie primär auf staatsschutzrechtliche Schutzobjekte ausgerichtet. Eine Zuordnung des BSI zum Kreis der Produzenten von Geheimdienstinformationen scheidet folglich aus.

Ebenso verhält es sich mit den Einrichtungen des GTAZ und des GIZ. Zwar handelt es sich in beiden Fällen um einen Zusammenschluss verschiedener mit Terrorfragen befassten Sicherheitsbehörden,[197] jedoch verfügen weder das GTAZ noch das GIZ über eigenständige Überwachungskompetenzen. Die beteiligten Behörden werden selbstständig und nur unter Rückgriff auf die ihnen jeweils zugewiesenen Kompetenzen tätig.[198] Das GTAZ und das GIZ sind damit jeweils ein Kooperationsforum der verschiedenen Sicherheitsbehörden und keine Produzenten von Geheimdienstinformationen i.S.d. der gewählten Definition.[199]

C. Zwischenergebnis zu Produzenten

Bei der Suche nach Produzenten von Geheimdienstinformationen in der deutschen Sicherheitsarchitektur wurden verschiedene Sicherheitsbehörden diskutiert. Im Rahmen der Untersuchung konnten neben den klassischen Diensten mit dem BKA und ZKA weitere Behörden herausgearbeitet werden, denen der Einsatz quasi-nachrichtendienstlicher Instrumentarien und damit die Produktion von Geheimdienstinformationen gestattet ist. Sowohl das ZKA als auch das BKA erfüllen jedoch nur Teilaspekte der Geheimdienstdefinition. Die klassische Trias aus BfV, BND und MAD produziert in der deutschen Sicherheitsarchitektur nach wie vor den größten Anteil an Geheimdienstinformationen, und wird als Modell für den deutschen Sicherheitssektor herausgegriffen. Der Fokus liegt dabei vor allem auf dem BfV sowie ergänzend dem BND. Eine gesonderte Darstellung des MAD ist aufgrund der starken Anlehnung des MADG an das BVerfSchG nicht erforderlich.

---

[196] Dafür spricht die die Formulierung unter „Wer sind unsere Kunden“ auf der offiziellen Internetseite des BSI, www.bsi.bund.de/DE/DasBSI/Leitbild/leitbild_node.html [Stand: 24.3.2011].

[197] Vertiefend zum GTAZ und dem GIZ *Droste,* Handbuch, S. 580ff; *Klee,* S. 112ff, 117ff, 145ff; *Zöller,* JZ 2007, S. 767ff.

[198] Vgl. *Klee,* S. 115.

[199] So etwa die Homepage des Bundesministeriums des Inneren unter www.bmi.bund.de/DE/Themen/Sicherheit/Terrorismus/NatZusammenarbeit/NatZusammenarbeit.html?nn=303936, ebenso *Klee,* S. 113.

III. Auswirkungen der deutschen Sicherheitsarchitektur

Die Verortung der Geheimdienste in die Sicherheitsarchitektur kann die strafprozessuale Nutzung von Geheimdienstinformationen maßgeblich beeinflussen. Die nachfolgenden Ausführungen geben zunächst einen Überblick über die Entwicklung der Sicherheitsarchitektur (A.). Im Anschluss daran werden die Auswirkungen dieser Sicherheitsarchitektur auf die Nutzung von Geheimdienstinformationen untersucht (B.).

A. Entwicklung der Sicherheitsarchitektur

Das Verhältnis der deutschen Nachrichtendienste zu den Strafverfolgungsbehörden hat zahlreiche Entwicklungsstufen durchlaufen. Nachfolgend werden die für die heutige Verortung der Dienste maßgeblichen Entwicklungslinien von der Nachkriegszeit bis in die Gegenwart nachgezeichnet.[200] Zur Entwicklung des Nachrichtendienstwesens bis 1945 sei auf die einschlägige Literatur verwiesen.[201]

1. Ausgangslage nach 1945

Nach dem Ende des zweiten Weltkrieges wurde das deutsche Sicherheitswesen neu geordnet. Die Neustrukturierung war maßgeblich durch das Trennungsgebot geprägt, welches im Polizeibrief der Alliierten vom 14. April 1949 und dem sich anschließenden Genehmigungsschreiben zum Grundgesetz vom 2. Mai 1949 zur Bedingung für die Schaffung eines Nachrichtendienstwesens gemacht wurde.[202] In den maßgeblichen Textpassagen wurden der Bundesrepublik Deutschland die Einrichtung von Polizeibehörden sowie die Schaffung einer Stelle zur Sammlung und Verbreitung von Auskünften über umstürzlerische Tätigkeiten gegen die Bundesregierung gestattet.[203] Letzteres gab die Ermächtigung zur Errichtung der heutigen Nachrichtendienste. Wesentliches Kernelement war jedoch der Verzicht dieser

---

[200] Vertiefend zur Entwicklung *König,* Kapitel 1 und 2.

[201] Vertiefend zu den historischen Grundlagen *Droste,* Handbuch S. 1ff; *König*, S. 49ff.

[202] Dieser Brief erging an den Präsidenten des Parlamentarischen Rates in der Endphase der Beratungen zum Grundgesetz; vgl. insgesamt *Klee,* S. 38ff; *Singer,* OK, S. 81ff; *Singer*, Die Kriminalpolizei 2006, S. 85ff.

[203] Vgl. *Albert,* ZRP 1995, S. 106. Zu diesem Zeitpunkt bedurfte die Errichtung von Bundesbehörden aufgrund Vorbehaltsrechte der Alliierten zunächst deren Zustimmung. Der vollständige Wortlaut ist abgedruckt bei *Singer,* OK, S. 81f, in englischer Sprache bei *Roewer,* S. 135 Fn. 197.

Stellen auf Polizeibefugnisse.[204] So sollte einerseits dem staatlichen Bedürfnis nach einer frühzeitigen Aufklärbarkeit umstürzlerischer Bewegungen Rechnung getragen werden, andererseits sollten die Einschränkungen das erneute Aufkommen einer unkontrollierbaren Zentralgewalt i.S.d. Gestapo verhindern.[205] Durch die Vorgaben sollte eine Bündelung von Überwachungs- und Exekutivbefugnissen von vorneherein ausgeschlossen werden. Das deutsche Nachrichtendienstwesen wurde dementsprechend nach dem Vorbild des britischen *Security Service* ohne Exekutivbefugnisse ausgestattet und dem Trennungsgebot unterworfen.[206]

Über den ausdrücklichen Wortlaut des Polizeibriefes hinaus sollte das Trennungsgebot die Gestaltung des Nachrichtendienstwesens in mehrerlei Hinsicht regeln.[207] Auf einer ersten Ebene fordert das Trennungsgebot eine befugnisrechtliche Trennung.[208] Danach ist den Diensten der Einsatz polizeilicher Maßnahmen, wie etwa Festnahmen, Durchsuchungsmaßnahmen, Personenüberprüfungen und Beschlagnahmungen, untersagt.[209] Sie dürfen weder zur Informationsbeschaffung noch zur Durchsetzung sonstiger Anliegen traditionelle Zwangsmaßnahmen anwenden.[210] Selbst ein entsprechendes Ersuchen ist unzulässig. Diese Exekutivbefugnisse sind der Polizei vorbehalten, welche im Gegenzug dem Bürger bei ihrem Einsatz grundsätzlich offen gegenübertreten muss.[211] Auf einer zweiten Ebene schreibt das Trennungsgebot eine organisatorische beziehungsweise personelle Trennung von Polizei und Verfassungsschutz vor. Diese bis heute geltende Komponente verbietet sowohl eine behördliche Vereinigung, als auch eine gegenseitige personelle Angliederung von Verfassungsschutz und Polizei.[212] Das Trennungsgebot in seiner Grundkonzeption beinhaltet als zentrale Elemente somit eine grundsätzliche Trennung von nachrichtendienstlichen und polizeilichen Behörden, Personal und Methoden.[213] Diese Elemente des Trennungsgebots wurden für den

---

[204] Zu diesen Befugnissen zählen insbesondere die polizeilichen Exekutivmaßnahmen in Form der Standardbefugnisse sowie die zwangsweise Durchsetzung von Verwaltungsakten, vgl. *Soiné,* NStZ 2007, S. 248.

[205] Vgl. hierzu insgesamt *Albert,* ZRP 1995, S. 106; Borgs-Maciejewski/Ebert-*Borgs*, § 3 BVerfSchG Rn. 134; *Roewer,* § 3 Rn. 191; *Singer*, Die Kriminalpolizei 2006, S. 86.

[206] Vgl. *Albert,* ZRP 1995, S. 106; *Droste*, Handbuch, S. 17f; *Singer*, Die Kriminalpolizei 2006, S. 86.

[207] Siehe vertiefend zum Inhalt des Trennungsgebots *Albert*, ZRP 1995, S. 105 ff; *Baumann*, DVBl 2005, S. 800ff; *Singer*, Die Kriminalpolizei 2006, S. 87ff; *Wolff*, DöV 2009, S. 60ff.

[208] Vgl. *Roewer,* § 3 Rn. 199ff.

[209] Siehe zur Aufzählung *Singer*, Die Kriminalpolizei 2006, S. 87.

[210] Vgl. *Droste,* Handbuch, S. 295.

[211] Vgl. *Albert,* ZRP 1995, S. 106; *Werthebach/Droste-Lehnen,* ZRP 1994, S. 63.

[212] Vgl. *Wolff,* DöV 2009, S. 601.

[213] Die daneben geführte Diskussion um die rechtliche Qualität bzw. den Verfassungsrang des Trennungsgebots ist für die vorliegende Fragestellung nicht von Relevanz. Sie kommt höchstens bei einer Neuregelung oder Abschaffung des Trennungsgebots zum Tragen. Vgl. zur überwiegenden Ablehnung des Verfassungsrangs *Baumann,* DVBl 2005,

Verfassungsschutz erstmals im Jahre 1950 im Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes vom 28.9.1950, dem heutigen BVerfSchG, gesetzlich fixiert.[214] Das Gesetz beschränkte sich insofern auf die absolut notwendigen Regelungen.[215]

Daneben wurden die Nachrichtendienste mit der Entstehung des Grundgesetzes erstmals ausdrücklich in die föderale Struktur des deutschen Rechtssystems integriert. Zwar konnte Deutschland bereits vor 1949 auf eine lange Tradition föderaler Strukturen zurückblicken. Mit der Schaffung des Grundgesetzes wurde dieses Organisationsprinzip allerdings erstmals verfassungsrechtlich festgeschrieben. In diesem Gefüge ist zwischen gefahrenabwehrenden (präventiven) und strafverfolgenden (repressiven) Aufgaben zu unterscheiden. Die Nachrichtendienste können zusammen mit der Polizei[216] grundsätzlich der Prävention zugeordnet werden, wohingegen repressive Aufgaben von den Strafverfolgungsbehörden wahrgenommen werden.[217] Zwischen geheimdienstlicher Prävention und der strafrechtlichen Ahndung sollten im Ausgangspunkt keine Überschneidungsbereiche bestehen.[218] Für die Einordnung der Dienste resultierte hieraus zunächst eine Verbannung aus dem Bereich der Strafverfolgung.

Die durch die genannten Ordnungsprinzipien bewirkte ursprünglich klare Abtrennung des Nachrichtenwesens vom Polizei- und Strafverfolgungssektor hat verschiedene Entwicklungsstufen durchlaufen.

2. Entwicklung der Sicherheitsarchitektur bis heute

Eine erste Annäherung erfolgte in den 70er und 80er Jahren des 20. Jahrhunderts. Diese Zeit war durch eine Zunahme an ausländer- und linksextremistischen Gewalttaten sowie einer steigenden Drogenkriminalität geprägt.[219] Der Gesetzgeber versuchte dieser wachsenden Bedrohung durch ein Konzept der inneren Sicherheit entgegenzuwirken.[220] Die als Reaktion erlassenen Sicherheitspakete aus

---

S. 801ff; *Droste*, Handbuch, S. 14ff; *Klee,* S. 48ff; *Singer,* OK, S. 92ff; *Singer*, Die Kriminalpolizei 2006, S. 112ff.

214 Die Mehrheit der genannten Dimensionen des Trennungsgebots beanspruchen in den §§ 1 I 2, 2 III 1 BNDG, §§ 2 I 3, 8 III BVerfSchG, §§ 1 IV, 4 II MADG bis heute Geltung.

215 Vgl. *Droste,* Handbuch, S. 11; *Singer*, Die Kriminalpolizei 2006, S. 86.

216 Die Polizeihoheit liegt nach Art. 30, 70, 83 GG grundsätzlich bei den Bundesländern. Die Polizeibehörden nehmen als Hilfsbeamte der Staatsanwaltschaft zum Teil auch repressive Aufgaben wahr. Eine eindeutige Zuordnung eventuell doppelfunktionaler Maßnahmen entscheidet sich nach dem Schwerpunkt der objektiv erkennbaren Zwecksetzung des Eingriffs, vgl. Wabnitz/Janovsky-*Bär,* 25. Kap. Rn. 101.

217 Vgl. *Forkert-Hosser,* S. 30f.

218 Vgl. *Forkert-Hosser,* S. 27f spricht von einem Entweder-Oder-Verhältnis.

219 Beispiele sind das Olympia-Attentat von 1972 oder die Anschläge der RAF.

220 Vgl. hierzu *Engelhart,* in: Wade/Maljević, S. 505.

dem Jahr 1972 beinhalteten unter anderem ein Änderungsgesetz zum Verfassungsschutzgesetz, in dem die Zuständigkeiten des Verfassungsschutzes wesentlich erweitert wurden.[221] Weitere Änderungen zielten auf eine verbesserte Zusammenarbeit von Nachrichtendiensten, Polizei und den Strafverfolgungsbehörden, die Ausweitung des Beobachtungsauftrags des Verfassungsschutzes auf ausländerextremistische Bestrebungen sowie eine Verlagerung der Strafbarkeit in den Vorfeldbereich.[222] Insgesamt führten die Reformen des Sicherheitswesens zu einer verstärkten Vorverlagerung und Verbreiterung der Informationserhebung und damit zu einer schrittweisen Vernachrichtendienstlichung von Polizei und Strafverfolgungsbehörden.[223] Damit kam es erstmals zu einer teilweisen Vereinigung ursprünglich getrennter präventiver und repressiver Tätigkeitsfelder.

Eine Zäsur erfolgte mit dem Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983.[224] Darin wurde in Bezug auf personenbezogene Daten das Recht auf informationelle Selbstbestimmung konkretisiert und die Notwendigkeit hinreichend klarer sowie verhältnismäßiger Eingriffsgrundlagen hervorgehoben. Der Gesetzgeber erkannte, dass die bisherigen nachrichtendienstlichen Rechtsgrundlagen den dort aufgestellten Anforderungen nicht genügten. Die daraufhin eingeleitete Reform des Nachrichtendienstrechts wurde erst im Jahre 1990 mit dem Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990 abgeschlossen. In diesem Zusammenhang wurden unter anderem das Bundesverfassungsschutzgesetz von 1950 reformiert und erstmals Rechtsgrundlagen für den BND und den MAD erlassen.[225]

Angestoßen durch die Vorgaben des Volkszählungsurteils wurden polizeiliche und nachrichtendienstliche Aufgaben und Arbeitsfelder in den einzelnen Ermächtigungsgrundlagen klar voneinander abgrenzt. Hierdurch wurde die im Trennungsgebot angelegte Aufteilung zwischen Polizei und Verfassungsschutz durch eine dritte, funktionelle Komponente ergänzt.[226] Nach dieser dürfen sich polizeiliche und nachrichtendienstliche Aufgabenfelder zwar überschneiden, nicht jedoch mit-

---

[221] Vgl. das Gesetz zur Änderung des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes vom 7.8.1972, BGBl. I, 1972, S. 1382, sowie *Droste,* Handbuch, S. 18f.

[222] Vgl. *König,* S. 101. Zur Einführung etwa des § 129a StGB siehe BGBl. I, 1976, S. 2181. Darin wird die Bildung einer terroristischen Vereinigung unter Strafe gestellt.

[223] Vgl. *Hefendehl,* GA 2011, S. 218.

[224] BVerfGE 65, 1ff. Zu den Auswirkungen des Urteils auf das Nachrichtendienstwesen siehe *Droste,* Handbuch, S. 21ff; *Singer,* OK, S. 305ff.

[225] BGBl. I, 1990, S. 2954. Zu dieser „Totalreform" siehe *Droste,* Handbuch, S. 22f. Diese so geschaffenen Nachrichtendienstgesetze wiesen eine insgesamt höhere Regelungsdichte auf als die ursprüngliche Fassung des BVerfSchG von 1950.

[226] Vgl. *Albert,* ZRP 1995, S. 106.

einander identisch sein.[227] Eine dem Trennungsgebot entsprechende organisatorische Aufspaltung wäre überflüssig, wenn über eine parallele Aufgabenwahrnehmung polizeiliche Aufgaben unter Einsatz nachrichtendienstlicher Befugnisse wahrgenommen werden könnten.[228] Die Novellierung des Nachrichtendienstrechts führte im Nachgang des Volkszählungsurteils zu einer klaren Abtrennung nachrichtendienstlicher Zuständigkeiten und Aufgaben. Abgesehen von vereinzelt fixierten Übermittlungsregeln waren die Dienste im Übrigen nicht berechtigt, angefallene Zufallsfunde an die Strafverfolgungsbehörden zu übermitteln.[229] Aufgrund der ohnehin abweichenden Beobachtungsaufträge bestand für eine solche Übermittlung beziehungsweise Zusammenarbeit jedoch in den meisten Fällen von vorneherein kein Bedürfnis.

In den 80er und 90er Jahren kam es schließlich insgesamt zu einer Annäherung nachrichtendienstlicher, strafrechtlicher und polizeilicher Befugnisse. Im Zuge des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Formen der Organisierten Kriminalität vom 15. Juli 1992 wurden in die Strafprozessordnung mit den §§ 100c, 100d, 110a StPO nachträglich verdeckte und heimliche Ermittlungsmaßnahmen eingeführt.[230] Hierdurch wurde der ehemals den Diensten vorbehaltene Einsatz technischer Mittel und Verdeckter Ermittler auch offiziell dem Strafverfolgungssektor gestattet. Die Dienste erfuhren nach dem Ende des Ostblocks ebenfalls eine Neuausrichtung.[231] Durch das Verbrechensbekämpfungsgesetz von 1994 wurde der G10-Katalog zur strategischen Überwachung auf Kriminalitätsfelder wie den Terrorismus, Waffenhandel, Drogenhandel, Geldwäsche und damit zum Teil auf Delikte ohne jeglichen Bezug zum nachrichtendienstlichen Beobachtungsauftrag erweitert.[232] Hierdurch wurden den Diensten ehemals rein strafrechtliche Aufklärungsfelder zugänglich gemacht.[233] Daneben durften sie erstmals

---

[227] SächsVerfGH NVwZ 2005, S. 1310f, zur Regelung des Art. 83 III 1 GG der Sächsischen Verfassung. Diese Argumentationsstruktur ist auf das auf Bundesebene geltende Trennungsgebot übertragbar. Zudem *Droste,* Handbuch, S. 292.

[228] SächsVerfGH NVwZ 2005, S. 1310, 1312.

[229] Vgl. u.a. *Singer,* in: Jäger/Daun, S. 273f. Kritisch zur Informationshilfe u.a. *Denninger,* ZRP 1981, S. 232; *Lisken,* NJW 1982, S. 1486; *Nehm,* NJW 2004, S. 3294.

[230] Vgl. OrgKG vom 15.7.1992, BGBl. I, 1992, S. 1302. Es ist zwischen heimlichen und verdeckten Ermittlungen zu unterscheiden. Heimliche Ermittlungen sollen nicht bemerkt werden, verdeckte Ermittlungen verwenden Täuschungselemente.

[231] Vgl. *Singer,* in: Jäger/Daun, S. 271f.

[232] Erforderlich sei allerdings das Vorliegen einer außen- und sicherheitspolitischen Relevanz; vgl. insgesamt *Singer,* in: Jäger/Daun, S. 273f. Diese Erweiterung wurde vom BVerfG lediglich hinsichtlich der Geldfälschung und Geldwäsche beanstandet.

[233] Vgl. *Roggan,* in: Roggan/Kutscha, S. 432; *Singer,* in: Jäger/Daun, S. 274. Insbesondere dem Bereich des Drogenhandels kommt keine sicherheitspolitische Bedeutung zu. Die vom Gesetzgeber behauptete Bedrohung der Sicherheit und Funktionsfähigkeit des Staates genügt nach *Schaefer,* NJW 1999, S. 2572, nicht.

geheimdienstliche Zufallsfunde an die Strafverfolgungsbehörden weiterleiten.[234] Dies ermöglichte die Verknüpfung verdachtslos erhobener Daten mit einzelnen Individuen.[235] Eine Regelung, wie mit den übermittelten Daten im Rahmen des Strafverfahrens umzugehen sei, wurde allerdings nicht geschaffen.[236] Diese Entwicklung führten zu einer Vermischung präventiver und repressiver Aufgabenfelder sowie einer Überlappung geheimdienstlicher und polizeilicher Befugnisse. Insbesondere durch die Schaffung der Weitergabebefugnis hatte der Gesetzgeber einen Konnex zwischen dem Geheimdienst- und dem Strafverfolgungssektor hergestellt. Damit veränderte er nachdrücklich die Stellung der Dienste in der Sicherheitsarchitektur, ohne jedoch zu diesem Zeitpunkt das Verhältnis zur Strafprozessordnung zu regeln.[237] Hierdurch entstanden zahlreiche Unsicherheiten, die weniger durch das Trennungsgebot, als vielmehr die fehlendende Verfugung beider Bereiche bedingt waren.

In diesem Zusammenhang wird vor allem die Einbeziehung der Organisierten Kriminalität (OK) in den Beobachtungsauftrag vereinzelter Landesverfassungsschutzbehörden kritisiert.[238]

Die Befürworter dieser Ausweitung begründen die Einbeziehung der OK mit dem gesamtstaatlichen Bedrohungspotential dieser kriminellen Erscheinungsform, welche eine Einordnung als verfassungsfeindliche Bestrebung beziehungsweise Bedrohung der freiheitlichen demokratischen Grundordnung rechtfertige.[239] Demgegenüber handelt es sich nach Ansicht der Kritiker bei der OK primär um ein kriminelles Verhalten, das über eine Politik- und Gewinnorientierung hinaus weder eine besondere sicherheitspolitische Relevanz noch einen sonstigen Bezug zum Aufgabenkreis des Verfassungsschutzes aufweise.[240] Durch die Ausweitung des Beobachtungsauftrags würden die Nachrichtendienste ohne Bindung an die Straf-

---

[234] Kritisch *Riegel,* ZRP 1995, S. 177; *Roggan,* in: Roggan/Kutscha, S. 432; *Singer,* OK, S. 262f.

[235] So *Roggan,* in: Roggan/Kutscha, S. 434.

[236] Eine solche ist aber aus verfassungsrechtlichen Gesichtspunkten notwendig; vgl. *Singelnstein,* ZStW 120 (2008), S. 854; SK-StPO-*Wohlers,* § 161 Rn. 52, sowie jüngst den Beschluss des BVerfG vom 24.2.2012, 1 BvR 1299/05. Zur Verfassungswidrigkeit der bis dato bestehenden Rechtslage vgl. *P.-A. Albrecht,* StV 2001, S. 419.

[237] Eine solche Regelung wurde erst durch die Neuregelungen des § 161 II StPO im Jahr 2008 eingefügt; vgl. hierzu unter Teil 2, III.B.4.a)aa).

[238] Vgl. *Droste,* Handbuch, S. 54f; *Kühne,* Strafprozessrecht, Rn. 377; *Roggan,* in: Roggan/Kutscha, S. 414; *Singer,* in: Jäger/Daun, S. 275. Diese Ausdehnung erfolgte im hessischen, bayerischen, thüringischen sowie saarländischen Landesverfassungsschutzgesetz, vgl. z.B. Art. 1 I 2 BayVSG, Art. 3 I 1 Nr. 5 BayVSG oder § 1 SVerfSchG. Auf Bundesebene existiert eine derartige Kompetenz nur für den BND.

[239] So etwa *Droste,* Nachrichtendienste, S. 121.

[240] So etwa *Kühne,* Strafprozessrecht, Rn. 377; *Singer,* in: Jäger/Daun, S. 273, 276f. A.A. *Droste,* Handbuch, S. 55, die auf die tatsächlichen Auswirkungen der OK verweist.

prozessordnung an der Aufklärung normaler Straftaten beteiligt.[241] Dies sei bedenklich, wenn die Nachrichtendienste nicht lediglich zu strategischen Zwecken, sondern zur operativen Aufklärung im Einzelfall eingesetzt würden.[242] Ein solcher Aufgabenwandel verkenne nicht nur die Besonderheiten und Bedürfnisse des nachrichtendienstlichen Beobachtungsauftrags, sondern bringe zugleich die Zuständigkeitsverteilung zwischen den verschiedenen Sicherheitsbehörden durcheinander. Dies sah das Sächsische Verfassungsgericht in seinem Urteil vom 21. Juli 2005 ähnlich. Darin beschränken die Richter die Einbeziehung der OK in den Beobachtungsauftrag auf Fälle, die zugleich eine verfassungsgefährdende Tendenz aufweisen.[243] Die Beobachtung der OK war in verfassungskonformer Auslegung nach dem sächsischen Verfassungsschutzgesetz daher nur bei einer Bedrohung der freiheitlichen demokratischen Grundordnung, des Bestands oder der Sicherheit des Bundes oder der Länder gestattet.[244] Als Folge dieser Rechtsprechung wurde die OK aus dem Aufgabenkatalog des sächsischen Landesverfassungsschutzgesetzes wieder entfernt. In den übrigen Landesverfassungsschutzgesetzen ist die Beobachtung der OK zum Teil jedoch weiterhin enthalten. Daran anknüpfend verweisen manche Autoren darauf, dass bestimmte OK-Bereiche durchaus die Qualität einer verfassungsfeindlichen Bestrebung erreichen können. In diesem Fall begegne der Einsatz der Dienste solange keinen Bedenken, wie ihre Tätigkeit auf eine einzelfallunabhängige Strukturaufklärung begrenzt sei und dem Begriff der OK bei der verfassungsschutzrechtlichen Aufgabenwahrnehmung ein engeres Verständnis zugrunde liege.[245] Um eine Instrumentalisierung der Dienste zu Strafverfolgungszwecken zu verhindern, sei daher eine eindeutige Grenzziehung durch die Landesgesetzgeber erforderlich. Die Einbeziehung der OK sei insofern ausdrücklich auf solche Erscheinungsformen zu begrenzen, die zugleich die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder der Länder bedrohen.[246]

Mit den Terroranschlägen vom 11. September 2001 erfolgte ein weiterer Entwicklungssprung, durch den die Zusammenarbeit der Sicherheitsbehörden weiter

---

[241] So *Roggan,* Polizeistaat, S. 160f; *Singer,* in: Jäger/Daun, S. 276.

[242] Vgl. *Roggan,* Polizeistaat, S. 160f; *Singer,* in: Jäger/Daun, S. 276.

[243] So das Urteil des SächsVerfGH zum „Großen Lauschangriff", NVwZ 2005, S. 1310, 1312, sowie *Kutscha,* NVwZ 2005, S. 1233.

[244] Vgl. Urteil des SächsVerfGH, NVwZ 2005, S. 1310, 1. Leitsatz, sowie *Kutscha,* NVwZ 2005, S. 1233; *Soiné,* ZRP 2008, S. 108.

[245] Vgl. u.a. *Soiné,* ZRP 2008, S. 110f.

[246] Vgl. *Soiné,* ZRP 2008, S. 110f. Alternativ fordert *Graulich,* in: Graulich/Simon, S. 160f, die Dienste bei einem repressiven Tätigwerden den Vorgaben der StPO zu unterwerfen. In diesem Fall sei die parlamentarische Kontrolle durch justizielle Elemente, wie z.B. einem dem „in camera"-Senat des BVerwG angelehnten Fachsenat, zu ergänzen. Dieser sollte bei einem obersten Bundesgericht angesiedelt sein und unter Einhaltung strikter Geheimhaltungsregeln die Rechtmäßigkeit geheimdienstlicher Tätigkeiten überprüfen dürfen.

intensiviert wurde. Der internationale beziehungsweise islamistische Terrorismus rückte verstärkt in den Fokus des Gesetzgebers. In der Folge wurden zahlreiche Gesetzesvorhaben und Sicherheitspakete, wie das Terrorismusbekämpfungsgesetz (2002),[247] das Gemeinsame-Dateien-Gesetz (2006)[248] sowie das Terrorismusbekämpfungsergänzungsgesetz (2007)[249] verabschiedet. Die verschiedenen Regelwerke sollten die Kompetenzen der einzelnen Sicherheitsbehörden erweitern und die Zusammenarbeit und den Datenaustausch verbessern.[250] Auf der Grundlage der genannten Gesetze wurden beispielsweise neue Koordinierungsgremien geschaffen und gemeinsame Datenbanken ausgebaut. Beispielhaft sind an dieser Stelle die Schaffung des GTAZ im Jahr 2004 und des GIZ im Jahr 2007 sowie die Freischaltung der Anti-Terror-Datei (ATD) im Jahr 2007 zu nennen.[251] Das GTAZ wurde errichtet, um die operative Zusammenarbeit der Sicherheitsbehörden im Bereich des Terrorismus durch den Austausch und die Verknüpfung aktueller, sicherheitsrelevanter Informationen zu verbessern.[252] Der konkrete Erkenntnisaustausch wird mangels ausdrücklicher Errichtungsermächtigung auf die jeweils maßgeblichen Fachgesetze gestützt.[253] Teilnehmer sind insgesamt 40 Sicherheitsbehörden des Bundes und der Länder, die unter der Leitung des BKA und des BfV zusammenarbeiten.[254] Die Schaffung des GTAZ führt damit zu einer institutionellen Annäherung von Polizei und Verfassungsschutz. Allerdings wird versucht den Vorgaben des Trennungsgebots durch eine organisatorische Aufteilung in eine polizeiliche (PIAS) und eine nachrichtendienstliche (NIAS) Informations- und Analysestelle gerecht zu werden. Das GIZ ist der Konzeption des GTAZ weitgehend angenähert.[255] Ebenso wie dieses vereint es zahlreiche Vertreter der Nachrichtendienste sowie der Polizei- und Strafverfolgungsbehörden.[256] Inhaltlich werden im GIZ internetspezifische terroristische und extremistische Bestrebungen beobachtet und

---

[247] Sog. Sicherheitspaket 2, BGBl. I, 2002, S. 361; vgl. *Droste,* Handbuch, S. 24f.

[248] Sog. Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder, GDG, BGBl. I, 2006, S. 3409.

[249] BGBl. I, 2007, S. 3198.

[250] Vgl. *Kühne,* Strafprozessrecht, Rn. 377.1.

[251] Eingehend zur Zusammenarbeit von Polizei und Nachrichtendiensten *Klee,* S. 111ff.

[252] Dies erfolgt etwa durch tägliche Lagebesprechungen, gemeinsame Gefährdungsbewertungen und Strukturanalysen; vgl. *Klee,* S. 112; *Zöller,* JZ 2007, S. 767, sowie www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/Sicherheit/Terrorismus/GTAZ.html [Stand: 1.5.2012].

[253] Vgl. *Droste,* Handbuch, S. 582; *Klee,* S. 116.

[254] Vgl. *Droste,* Handbuch, S. 581; *Zöller,* JZ 2007, S. 768. Unter den Teilnehmern sind das BKA, das BfV der BND, die Bundespolizei, das ZKA, der MAD, das Bundesamt für Migration und Flüchtlinge, Vertreter des Generalbundesanwaltes sowie die jeweils 16 Landeskriminalämter und Landesämter für Verfassungsschutz.

[255] Vgl. *Klee,* S. 117f.

[256] Erfasst sind das BfV, das BKA, der BND, der MAD sowie der Generalbundesanwalt.

systematisch ausgewertet. Als drittes Beispiel wurde auf die ATD verwiesen. Hierbei handelt es sich um einen gemeinsamen Datenbestand beim BKA, in dem terrorismusbezogene Erkenntnisse der Polizei und des Verfassungsschutzes zusammengefasst werden.[257] Der Informationsfluss zwischen den zugriffsberechtigten Parteien wird mittels eines automatisierten Abrufverfahrens optimiert.[258] Die eigentliche Übermittlung richtet sich nach den spezialgesetzlichen Übermittlungsvorschriften. Der ATD liegt ein zweistufiges System zugrunde, das zwischen Grunddaten und erweiterten Grunddaten differenziert. Ergibt die Suchanfrage einen Treffer, so werden die Grunddaten unmittelbar angezeigt. Im Gegensatz dazu sind die erweiterten Grunddaten aus Gründen des Quellen- und Geheimdienstschutzes beim Abruf zunächst nicht unmittelbar sichtbar. Auf diese Daten kann nur im Eilfall[259] oder auf Nachfrage bei der speichernden Behörde zugegriffen werden. Diese Vorgaben dienen dazu, den Informationsaustausch zu begrenzen und zu vermeiden, dass verschiedene Sicherheitsbehörden identische Datenbestände anlegen.

Die beschriebenen Gremien und Datenverbunde gliedern die Nachrichtendienste damit über den punktuellen Datenaustausch hinaus in einen festen institutionellen und informationellen Rahmen ein. Diese Annäherungstendenzen dauern weiterhin an, was der Beschluss zum Aufbau einer dem ATD angelehnten „Verbunddatei Rechtsextremismus“ Anfang 2012 verdeutlicht.[260] Faktisch wird durch diese Entwicklung die bisherige Abschottung des Geheimdienstsektors aufgegeben. Das bisherige *need to know*-Prinzip, wonach sensible Informationen nur denjenigen Personen zur Verfügung gestellt werden, die sie auch tatsächlich dringend benötigen, wird weitgehend aufgegeben. Stattdessen wird nach dem *need to share*-Prinzip ein erleichterter und offensiver Wissensaustausch favorisiert.[261]

---

[257] Vertiefend *Droste,* Handbuch, S. 582ff; *Klee,* S. 145ff. Siehe zudem jüngst das BVerfG, 1 BvR 1215/07, welches bestimmte Teile der ATD für verfassungswidrig erklärt.

[258] Eingehend zu Inhalt, Grundlagen und Vereinbarkeit dieser Datenbestände mit dem Trennungsgebot vgl. *Klee,* S. 145ff. Zudem wurde die Einrichtung projektbezogener gemeinsamer Dateien gestattet, vgl. § 22a BVerfSchG, § 9a BNDG, § 9a BKAG. Dabei handelt es sich um befristete gemeinsame Projekte der Sicherheitsbehörden, die auch die Speicherung von Volltexten umfassen; vgl. *Klee,* S. 157ff; *Roggan/Bergemann,* NJW 2007, S. 878f.

[259] Ein solcher Eilfall wird bei einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder wenn es um eine Sache von erheblichem Wert geht, angenommen, sofern der Zugriff auf die Daten für die Vornahme einer Maßnahme unerlässlich ist; vgl. § 5 II ATDG.

[260] Vgl. den Gesetzesentwurf der Bundesregierung zur Verbesserung der Bekämpfung des Rechtsextremismus in BT-Drs. 17/8672. Hierbei handelt es sich um eine Reaktion auf die Anschläge der rechtsextremen Zwickauer Zelle. Vertiefend *Kutscha*, NVwZ 2013, S. 324ff.

[261] Vgl. *Jäger/Daun,* in: Borchert, S. 65; *Vorbeck,* in: Jäger/Daun, S. 299. Zu dieser allgemeinen Tendenz im europäischen Sektor ebenfalls *Storbeck,* in: Jäger/Daun, S. 157. Zur Notwendigkeit eines Wissensaustausches mit Blick auf den NSU-Skandal siehe *Gusy,* ZRP 2012, S. 231.

Diese Entwicklung wird zum Teil sehr kritisch gesehen.[262] Die Errichtung gemeinsamer Strukturen, Arbeitsabläufe und Datenbestände wird verschiedentlich als Schwächung der informationellen Trennung zwischen Polizei und Nachrichtendiensten empfunden.[263] Möglichkeiten, wie das automatisierte Abrufverfahren der ATD, gestatteten den Strafverfolgungsbehörden unabhängig von einer einzelfallbezogenen Übermittlung den Zugriff auf Vorfelddaten der Nachrichtendienste.[264] Die bei einer Suchanfrage erhaltenen Daten könnten insofern nicht nur zu Recherchezwecken, sondern nach § 6 I 2, IV ATDG zusätzlich für die Strafverfolgung genutzt werden.[265] Dieser ungehinderte Zugang zu nachrichtendienstlichen Erkenntnissen umgeht nach Ansicht vieler Kritiker den durch das Trennungsgebot bedingten Ausnahmecharakter eines Informationsaustausches.[266] Demgegenüber verweisen die Befürworter derartiger Datenbanken darauf, dass bestehende Informationsbeziehungen lediglich kanalisiert würden, ohne dass damit eine unzulässige Befugniserweiterung verbunden wäre.[267] So sei etwa der mit der ATD ermöglichte Informationsaustausch nicht schrankenlos, da bei einer Übermittlung nach § 6 I 2 ATDG neben den dort genannten Voraussetzungen zusätzlich die Bedingungen der nachrichtendienstlichen Übermittlungsvorschriften zu beachten seien.[268] Ebenso wenig bestehe eine direkte Zugriffsmöglichkeit.[269] Zudem sei eine Übermittlung nach § 6 IV ATDG mittelbar über die Sonderzuständigkeit des Generalbundesanwalts auf staatsschutzrelevante Sachverhalte begrenzt. Diese Bedenken werden im Wesentlichen im Urteil des Bundesverfassungsgerichts vom 24.4.2013 bestätigt. Das Bundesverfassungsgericht erklärt die ATD zwar in ihren Grundstrukturen als mit der Verfassung vereinbar, nicht jedoch in ihren einzelnen Ausgestaltungen.[270] Insbesondere die Beteiligungsmöglichkeiten anderer Behörden oder die Kriterien zur Erfassung bestimmter Personengruppen werden als Verstoß gegen den

---

[262] Vgl. *Roggan/Bergemann,* NJW 2007, S. 877; *Zöller,* JZ 2007, S. 770. In verfassungsrechtlicher Hinsicht wird vor allem eine unverhältnismäßige Beeinträchtigung des Rechts auf informationelle Selbstbestimmung bemängelt. Kritikpunkte sind neben dem Datenumfang, die umfassenden Speichermöglichkeiten sowie das Fehlen ausreichender Verwendungsregeln; vgl. *Klee,* S. 154; *Roggan/Bergemann,* NJW 2007, S. 878; *Zöller,* JZ 2007, S. 770. Jüngst auch *Kutscha,* NVwZ 2013, S. 324ff.

[263] Vgl. *Roggan/Bergemann,* NJW 2007, S. 877; *Zöller,* JZ 2007, S. 768.

[264] Vgl. insgesamt kritisch *Zöller,* JZ 2007, S. 771. A.A. bei *Droste,* Handbuch, S. 584, die darin einen wesentlichen Beitrag zur Wirksamkeit des Trennungsgebots sieht.

[265] Nach § 6 I 2 ATDG ist eine Verwendung zur Verfolgung einer besonders schweren Straftat zulässig, wenn die Daten erforderlich sind und die speichernde Behörde zustimmt. Daneben gestattet § 6 IV ATDG die Übermittlung der Daten an den Generalbundesanwalt zu Zwecken der Strafverfolgung.

[266] So etwa *Zöller,* JZ 2007, S. 770.

[267] Vgl. *Droste,* Handbuch, S. 584; *Klee,* S. 130ff, 148ff, 164ff.

[268] Vgl. § 7 ATDG.

[269] Vgl. *Weisser,* NVwZ 2011, S. 144.

[270] Vgl. BVerfG 1, 1215/07 vom 24.4.2013.

Bestimmtheitsgrundsatz und das Übermaßverbot gerügt. Allerdings dürfen die Vorschriften bis zu einer Neuregelung bis zum 31.12.2014 weiter angewendet werden.

3. Zwischenergebnis

Die Einordung der Dienste in die deutsche Sicherheitsarchitektur hat verschiedene Entwicklungsstufen durchlaufen. Die ehemals klaren Vorgaben des Trennungsgebots und des Sicherheitsföderalismus haben im Laufe der Entwicklungsgeschichte erheblich an Bedeutung eingebüßt.[271] Formal wird die Verortung der Nachrichtendienste zwar weiterhin durch die ursprünglichen Ordnungsprinzipien bestimmt, insgesamt jedoch verliert die ursprünglich strikte Zuordnung der verschiedenen Bereiche zunehmend an Deutlichkeit. Neben einer schrittweisen Annäherung des Geheim- und Polizeisektors wird eine Prioritätsverschiebung und Integration des deutschen Nachrichtendienstwesens deutlich.

B. Auswirkungen der Sicherheitsarchitektur auf die Informationsnutzung

Die Nachrichtendienste nehmen in der heutigen Sicherheitsarchitektur weiterhin eine Sonderstellung ein. Nachfolgend werden die Auswirkungen dieser Verortung auf die Nutzung von Geheimdienstinformationen dargestellt. In diesem Zusammenhang werden die Besonderheiten geheimdienstlicher Informationserhebung (1.), die Grenzen der Informationsnutzung (2.) sowie die wesentlichen Übermittlungsvorschriften (3.) und Verwertungsregeln (4.) erörtert. Die Darstellung beschränkt sich auf die für die vorliegende Fragestellung zentralen Charakteristika und versucht ein Grundverständnis für das vom deutschen Gesetzgeber gewählte Lösungsmodell zu schaffen. Es ist zu klären, inwieweit dieses Konzept durch die deutsche Sicherheitsarchitektur oder sonstige Einflussfaktoren bestimmt wird.

1. Besonderheiten geheimdienstlicher Informationserhebung

Die geheimdienstliche Informationserhebung zeichnet sich durch spezifische Besonderheiten aus. Die zentralen Merkmale werden primär anhand des BVerfSchG dargestellt. Dieses vermittelt über die Verweisungsnormen der §§ 4ff MADG und §§ 3ff BNDG die wesentlichen Besonderheiten der geheimdienstlichen Informationserhebung im deutschen Kontext. Auf relevante Besonderheiten nach dem

---

[271] So *Engelhart,* in: Wade/Maljević, S. 522. Für eine Vereinbarkeit mit dem Trennungsgebot *Droste,* Handbuch, S. 584; *Klee,* S. 130ff, 164ff. Ablehnend der Antrag der Fraktion DIE LINKE, in: BT-Drs. 16/2624; vgl. zudem Teil 2, III.B.5.a)aa).

BNDG und dem G10 wird bei Bedarf explizit eingegangen. Die charakteristischen Merkmale werden überwiegend im Vergleich zur Beweiserhebung durch die Polizei- und Strafverfolgungsbehörden dargestellt. Die im Einzelnen feststellbaren Unterschiede sind für die Beurteilung der Übermittlungs- und Verwertungsregeln von zentraler Bedeutung.

a) Geheimdienstliche Aufgaben und Aufklärungsrichtung

Die Aufgaben der deutschen Nachrichtendienste werden in den einzelnen Nachrichtendienstgesetzen festgelegt. Dies sind namentlich das BVerfSchG, das MADG und das BNDG. Das dort genannte Aufgabenspektrum wird durch das G10 nicht erweitert. Dieses regelt lediglich die Befugnisse für Eingriffe in Art. 10 GG, während sich die Aufgaben weiterhin an den Vorgaben der Nachrichtendienstgesetze orientieren.[272]

Den Nachrichtendiensten obliegt im Schwerpunkt die Beschaffung und Auswertung von Informationen über abstrakte Gefährdungen der inneren und äußeren Sicherheit.[273] Wie bereits bei der Darstellung des BfV angeführt, steht das Merkmal der Bestrebungen im Mittelpunkt der nachrichtendienstlichen Aufgabenwahrnehmung. Danach lässt sich die geheimdienstliche Beobachtungstätigkeit in zentralen Bereichen von der repressiven Zielsetzung der Strafverfolgungsbehörden abgrenzen. Den Diensten obliegt ein langfristig angelegter, zukunftsbezogener Beobachtungsauftrag. Das beobachtete Verhalten muss weder strafbar noch rechtswidrig sein, sofern diesem objektiv eine entsprechende politische beziehungsweise schädigende Wirkung zukommt.[274] Der Verzicht auf das Element der Rechtswidrigkeit wird anhand der sprachlichen Differenzierung innerhalb des § 3 I Nr. 1 BVerfSchG deutlich. Anders als bei der Beeinträchtigung nach Alt. 2 fehlt in Bezug auf die Bestrebung nach Alt. 1 der Zusatz der „Ungesetzlichkeit".[275] Staatsgefährdende Bedrohungslagen dürfen damit in einem nicht strafbewehrten Vorfeld beobachtet werden, um potentiell gefährliche Verflechtungen beziehungsweise staatsgefährdende Tendenzen aufdecken und Risikoeinschätzungen erstellen zu können.

Im Vergleich dazu müssen sich strafrechtliche Ermittlungen auf „verfolgbare Straftaten" i.S.d. § 152 II StPO beziehen. Die Strafverfolgungsbehörden sind damit anders als die Geheimdienste auf einen konkreten, in der Vergangenheit liegenden

---

272 Vgl. § 1 I G10 sowie *Singer,* OK, S. 266.

273 Vgl. *Hefendehl,* GA 2011, S. 212; *Weßlau,* S. 225. Eine Übersicht zu den nachrichtendienstlichen Kernaufgaben findet sich bei *Droste,* Nachrichtendienste, S. 101.

274 Vgl. Borgs-Maciejewski/Ebert-*Borgs*, § 3 BVerfSchG Rn. 9; *Gusy,* StV 1995, S. 323f; *Gusy,* GA 1999, S. 326; *Gusy,* ZRP 2012, S. 231; *Ostheimer,* S. 77; *Rödder,* S. 105; *Singer,* OK, S. 63. Allerdings wird die Gesetzeswidrigkeit oftmals vorliegen.

275 Vgl. *Singer,* OK, S. 163; *Droste,* Nachrichtendienste, S. 101, 168.

strafbaren Sachverhalt angewiesen, um tätig werden zu können.[276] Demgegenüber ist für ein Tätigwerden der Dienste nicht erforderlich, dass jemand durch die Begehung einer Straftat individuell einen Anlass gesetzt hat. Der tatbezogene Ansatz der Strafverfolgungsbehörden wird im Geheimdienstrecht durch einen organisationsbezogenen Beobachtungsauftrag ersetzt.[277] Umgekehrt hat der strafrechtliche Tatbezug den Vorteil, dass sämtliche strafbaren Verhaltensweisen einbezogen werden können.[278] Es existiert weder eine Beschränkung auf staatsschutzrelevante Bereiche noch auf zielgerichtete Verhaltensweisen. Aufgaben und Aufklärungsrichtung der Nachrichtendienste unterscheiden sich damit in zentralen Bereichen von denen der Strafverfolgung. Lediglich im Bereich der Staatsschutzstrafsachen sind thematische Überschneidungen denkbar. Eine Aufgabenidentität oder ein Konkurrenzverhältnis ist damit indes nicht verbunden.[279]

Daneben können die Aufgaben der Dienste von der präventiv-polizeilichen Gefahrenabwehr unterschieden werden. Die Polizei soll tatsächliche Gefahren für die öffentliche Sicherheit und Ordnung aktiv abwehren. Dagegen fokussiert das Nachrichtendienstwesen auf die Informationserhebung und die Beobachtung staatsschutzgefährdender Vorgänge.[280] Damit sind die Nachrichtendienste als Folge des Trennungsgebots auf einen eher passiven Beobachtungsauftrag beschränkt. Anders als die Polizeibehörden können sie potentielle beziehungsweise tatsächliche Gefahrenquellen gerade nicht durch aktive Zwangsmaßnahmen bekämpfen, sondern sind auf die Mitwirkung anderer Behörden angewiesen.[281]

Theoretisch können die nachrichtendienstlichen Aufgaben eindeutig von denen anderer Sicherheitsbehörden abgegrenzt werden.[282] Diese klassische Aufteilung wird vom Gesetzgeber jedoch zunehmend infrage gestellt – eine Tendenz, die vor allem an der vielfach diskutierten Ausdehnung auf den Bereich der Organisierten Kriminalität (OK) verdeutlicht werden kann, welche sich in Verfassungsschutzgesetzen einzelner Bundesländer finden lässt.[283] Diese wird vielfach als zu weit kritisiert, da hiermit eine unzulässige Ausdehnung des Beobachtungsspektrums auf

---

[276] Vgl. *Bertram,* S. 314; *Forkert-Hosser,* S. 26; *Gärditz,* S. 46; *Kramer,* Rn. 4.

[277] Vgl. *Kornblum,* S. 52.

[278] Zum Tatbezug bei strafrechtlichen Ermittlungen KK-*Schoreit,* § 152 Rn. 13.

[279] Vgl. *Rödder,* S. 106; *Singer,* OK, S. 330. Zur gemeinsamen Aufgabe, die wehrhafte Demokratie aufrechtzuerhalten, vgl. *T. Wollweber,* S. 99ff.

[280] *Lisken/Denninger,* in: Lisken/Denninger/Rachor, S. 114; *Ostheimer,* S. 75; *Rödder,* S. 105f; *Thamm,* in: Hirschmann/Leggemann, S. 238.

[281] Vgl. *Lisken/Denninger,* in: Lisken/Denninger/Rachor, S. 114.

[282] Zur Vermeidung von Doppelzuständigkeiten aus Effektivitätsgründen siehe *Gusy,* ZRP 2012, S. 231.

[283] Vgl. *Roggan,* in: Roggan/Kutscha, S. 414; vgl. beispielsweise in Art. 1 I 2 BayVSG, Art. 3 I 1 Nr. 5 BayVSG (Bayerisches Verfassungsschutzgesetz) oder § 1 SVerfSchG (Saarländisches Verfassungsschutzgesetz). Zur Diskussion *Remmele,* in: Bundesministerium des Inneren, Verfassungsschutz, S. 328; *Soiné*, ZRP 2008, S. 106ff.

Erscheinungsformen klassischer Kriminalitätsfelder verbunden sei.[284] Überwiegend wird dem Begriff der OK im Nachrichtendienstwesen daher ein engeres Begriffsverständnis zugrunde gelegt.[285] Danach ist die Beobachtung der OK durch den Verfassungsschutz nur gestattet, wenn diese zugleich die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder der Länder bedroht.[286] Für eine Beobachtungstätigkeit des Verfassungsschutzes müssen folglich stets ergänzend die klassischen Voraussetzungen der nachrichtendienstlichen Aufgabenbeschreibung vorliegen.[287] Eine entsprechende Begrenzung sei notfalls im Wege einer verfassungskonformen Auslegung hineinzulesen.[288] Als Argument wird angeführt, dass andernfalls die strategische Beobachtung staatsgefährdender Bestrebungen durch eine systemfremde, operative Aufklärung strafrechtlich relevanter Sachverhalte ersetzt würde. Ohne eine Bindung an ein staatsgefährdendes Potential würde es sich bei der OK lediglich um „materiell motivierte Kriminalität" handeln, die keine Zuständigkeit der Nachrichtendienste begründen könne.[289] Deren Einsatz sei erst bei Vorliegen einer gesamtstaatlichen Bedrohung gerechtfertigt.

Diese Diskussion verdeutlicht die allgemeine Tendenz, bislang klassische Kriminalitätsphänomene dem Beobachtungsspektrum der Nachrichtendienste zuzuordnen. Diese Ausweitung ist solange unproblematisch, wie die überwachten Vorgänge eine nachrichtendienstliche Relevanz aufweisen und diese den Diensten zu Zwecken einer Strukturaufklärung zugewiesen werden.[290] Die Unterscheidbarkeit von Aufgaben anderer Sicherheitsbehörden wird erst dann infrage gestellt, wenn die strategische Ausrichtung des geheimdienstlichen Beobachtungsauftrags zugunsten operativer Funktionen mit Einzelfallbezug aufgegeben wird. Bisher besteht jedoch weder zu Maßnahmen der polizeilichen Gefahrabwehr noch zu strafverfolgenden Aufgaben ein Konkurrenzverhältnis. Die Dienste sind entweder über die Art der Aufgabenwahrnehmung, das heißt ihrem bloß passiven Beobachtungs-

---

284 Vgl. zur Kritik *Roggan,* Polizeistaat*,* S. 160f.

285 So etwa SächsVerfGH NVwZ 2005, 1310, 1312ff; vgl. ergänzend *Kutscha,* NVwZ 2005, S. 1233; *Singer,* in: Jäger/Daun, S. 273ff; *Vorbeck,* in: Jäger/Daun, S. 298.

286 Kritisch *Denninger*, KritV 1994. S. 235; *Gusy*, StV 1995, S. 320ff; *Gusy*, GA 1999, S. 319ff; *Koch*, ZRP 1995, S. 24. Eine Zuständigkeit befürwortend *Droste*, Handbuch, S. 204; *Soiné,* ZRP 2008, S. 110.

287 Die Richter stützen sich auf die im Verfassungstext aufgeführten Schutzgüter. Danach sei ein Verstoß gegen Art. 83 III 1 SächsVerf gegeben, welcher die Zuständigkeit des Landesamtes auf die in Art. 73 Nr. 10b GG genannten Schutzgüter beschränkt.

288 Diese Auslegung stehe im konkreten Fall mit dem Willen des Gesetzgebers im Einklang, da dieser dem Fehlen des Zusatzes keine inhaltliche, sondern lediglich redaktionelle Bedeutung beimisst, vgl. SächsVerfGH NVwZ 2005, S. 1312, 1313. Zur zweifelhaften Motivationslage des bayerischen Landesgesetzgebers vgl. LT-Drs. 12/15217, S. 6, sowie *Roggan,* in: Roggan/Kutscha, S. 421. Die Beauftragung des bayerischen Verfassungsschutzes habe demnach den Vorteil, dass dieser nicht den Beschränkungen der StPO unterworfen sei.

289 Vgl. *Singer,* OK, S. 331.

290 Vgl. *Soiné,* ZRP 2008, S. 110f.

auftrag, oder die Zielsetzung, das heißt keine konkrete Gefahrenabwehr oder einzelfallbezogene Strafverfolgung, von den Aufgaben sonstiger Sicherheitsbehörden abgrenzbar. Trotz verschiedener Annäherungstendenzen beanspruchen die Gestaltungsvorgaben der deutschen Sicherheitsarchitektur damit weiterhin Geltung.

b) Geheimdienstliche Erhebungsbefugnisse

Zur Erfüllung ihres Beobachtungsauftrags dürfen die deutschen Nachrichtendienste verschiedene Methoden der Informationsbeschaffung einsetzen.[291] Die Ermittlungsbefugnisse orientieren sich primär am Modell des BVerfSchG, das direkt oder vermittelt über Verweisungsnormen für die Bundesnachrichtendienste gilt. Ausgangspunkt ist die Generalermächtigung in § 8 BVerfSchG, welche in den §§ 9ff BVerfSchG um weitere Befugnisse ergänzt wird.[292] Zusätzliche Spezialbefugnisse für Eingriffe in das Brief-, Post- und Fernmeldegeheimnis finden sich im G10.

Die Nachrichtendienste können auf unterschiedliche Erhebungsmethoden zurückgreifen. Eine erste Kategorie umfasst den Einsatz schlichter Erhebungsmaßnahmen. Diese Möglichkeit wird in § 8 I BVerfSchG eröffnet und betrifft die Erhebung aus öffentlich, das heißt allgemein zugänglichen Quellen wie Zeitungen und Webdiensten.[293] Eine zweite Kategorie bilden Methoden der heimlichen, untechnischen Informationsbeschaffung.[294] Innerhalb dieser Kategorie werden die Informationen etwa durch das Öffnen von Postsendungen, die Beobachtung oder die Befragung von Zielpersonen unter Verheimlichung der wahren Identität beschafft. Eine dritte Kategorie gestattet den Nachrichtendiensten den Einsatz von Vertrauenspersonen oder Verdeckten Ermittlern. Diese Personen werden für längere Zeit in ein Milieu eingeschleust, um gezielt Informationen über Personen oder Organisationen zu generieren.[295] Eine vierte Kategorie betrifft die Informationsbeschaffung unter Einsatz technischer Hilfsmittel. Die Informationen werden mittels Fotoaufnahmen, Abhör- und Filmaufzeichnungen von Telefonaten oder Verhaltensweisen oder dem Zugriff auf sonstige Datenbestände erhoben. In diese Kategorie fallen unter anderem die Auskunftsverlangen nach § 8a BVerfSchG, die optische wie akustische Wohnraumüberwachung und der Einsatz des IMSI-Catchers nach § 9 BVerfSchG.[296] Ebenfalls erfasst sind die individuelle und die strategische Überwachung nach dem G10.

---

[291] Eine Übersicht findet sich bei *Droste,* Nachrichtendienste, S. 103.

[292] Vgl. *Droste,* Handbuch, S. 224, 227.

[293] Vgl. *Droste,* Handbuch, S. 227. Für den BND findet sich die entsprechende Ermächtigung in § 2 BNDG.

[294] Vgl. *Singer,* OK, S. 286.

[295] Vgl. u.a. § 8 II 1 BVerfSchG gegebenenfalls i.V.m. § 4a MADG, § 3 BNDG.

[296] Gegebenenfalls i.V.m. § 5 MADG, § 3 Satz 2 BNDG.

Die letztgenannte Kategorie bedarf aufgrund der damit verbundenen Eingriffsintensität einer gesonderten Erläuterung. Die Auskunftsverlangen nach § 8a II BVerfSchG i.V.m. § 9 VI 1 BVerfSchG gestatten den Diensten den umfassenden Zugriff auf Verkehrs- und Bestandsdaten privater Unternehmen.[297] Erfasst werden unter anderem Auskünfte über Flugbuchungen und Kontodaten bei zentralen Stellen sowie Anfragen bei Luftfahrtunternehmen (Nr. 1) sowie Kredit- und Finanzdienstleistungsinstituten (Nr. 2). In diesem Zusammenhang können der Name und die Anschrift eines Kunden, Informationen zur Inanspruchnahme und den Umständen von Transportleistungen sowie Auskünfte zu Konten, Kontoinhabern, Geldbewegungen, Geldanlagen, insbesondere Kontostand und Zahlungsein- und -ausgänge erfragt werden. Die Einräumung dieser Befugnis soll den Diensten eine möglichst umfassende und frühzeitige Kenntnis über Reisewege, Ruhe- und Vorbereitungsräume sowie Zielgebiete internationaler terroristischer Gruppen oder anderer Personen verschaffen.[298] Die in der Vorschrift genannten Stellen sind nach § 8b VI BVerfSchG zur Auskunft verpflichtet.[299] Die Dienstleister können sich daher beispielsweise nicht auf das Bankgeheimnis berufen.[300] Ebenfalls im Anwendungsbereich des § 9 BVerfSchG fällt der Einsatz des IMSI-Catchers nach Abs. 4. Dabei handelt es sich um ein technisches Gerät, das die Basisstation eines Mobilfunknetzes simuliert. Die im Umfeld vorhandenen, empfangsbereiten Mobiltelefone melden sich bei dieser vermeintlichen Funkzelle an und übermitteln die einzigartige Kartenkennung des Mobiltelefons, die sogenannte *International Mobile Subscriber Identity*. Hierdurch kann eine relativ zielgenaue Ortung des Mobiltelefons vorgenommen werden.[301]

Ebenfalls in die vierte Kategorie fallen die nach dem G10 gestatteten Überwachungsmaßnahmen.[302] Das G10 unterscheidet zwischen individuellen und strategischen Eingriffen in das durch Art. 10 GG geschützte Brief-, Post- und Fernmeldegeheimnis. Die individuelle Überwachung richtet sich nach §§ 1 I, 3 I G10 und steht den Verfassungsschutzbehörden des Bundes und der Länder, dem MAD und dem BND zur Verfügung. Danach dürfen unter anderem die Inhalte eines aktuell

---

297 Gegebenenfalls i.V.m. § 2a BNDG; vgl. insgesamt *Zöller,* JZ 2007, S. 766. Diese Befugnisse wurden zuletzt mit Wirkung zum 10.1.2012 durch das Gesetz vom 7.12.2011, BGBl. I, 2011, S. 2576, reformiert, vgl. BT-Drs. 17/7513, 17/6925. Kritisch *Kutscha,* NVwZ 2013, S. 324, der darin eine polizeiähnliche Befugnis sieht.

298 BT-Drs. 17/6925, S. 12.

299 Diese gesetzlich normierte Pflicht soll klarstellen, dass die auskunftsgebenden Stellen nicht aufgrund eines etwaigen Vertragsbruches zu Schadensersatz verpflichtet sind.

300 Vgl. *Rehbein,* S. 46.

301 Hierzu ausführlich *Harnisch/Pohlmann,* NVwZ 2009, S. 1328ff; *Droste,* Handbuch, S. 328ff. Im Jahr 2009 wurden 93 derartiger Auskunftsverlangen und IMSI-Catcher-Einsätze vor allem durch das BfV durchgeführt, vgl. BT-Drs. 17/4277, S. 3ff. In den Bundesländern kam es zu 48 derartigen Auskunftsverlangen, vgl. BT-Drs. 17/4277, S. 8f.

302 Siehe vertiefend *Roggan*, G10, § 3 Rn. 1ff, § 5 Rn. 1ff.

stattfindenden Telekommunikationsvorgangs überwacht und aufgezeichnet werden.[303] Die Maßnahme dient folglich der Überwachung konkreter Einzelpersonen.[304] Daneben existiert die sogenannte strategische Telekommunikationsüberwachung nach §§ 1 II, 5 I G10. Diese ist ausschließlich dem BND vorbehalten. Sie gestattet die maschinelle Ausfilterung von Telekommunikationsvorgängen des internationalen Telekommunikationsverkehrs mittels bestimmter Suchbegriffe. Seit der Gesetzesnovelle 2001 ist die strategische Überwachung nicht mehr auf die nicht leitungsgebundene Telekommunikation, das heißt den Satelliten- und Richtfunkverkehr begrenzt, sondern erstreckt sich auf den gesamten internationalen Telekommunikationsverkehr. Hiervon wird die zwischen Deutschland und dem Ausland stattfindende Telekommunikation erfasst.[305] Wird in einem Gespräch eines der zugelassenen Stichworte verwendet, führt dies zu einer automatischen Aufzeichnung.[306] Als strategische und nicht gezielte Überwachung ist eine Individualisierung der Daten grundsätzlich unzulässig.[307] Bei der überwachten Kommunikation muss es sich daher um eine „gebündelte Übertragung" handeln.[308] Zudem dürfen die Suchbegriffe keine Identifikationsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen können.[309] Die strategische Überwachung bezweckt folglich nicht die Kontrolle einzelner Personen oder Taten, sondern die anlassunabhängige Telefonüberwachung zum Erhalt abstrakter Anhaltspunkte für Gefährdungslagen für die Bundesrepublik Deutschland.[310] Lediglich im Ausnahmefall kann eine Individualisierung nach § 5 II 2 G10 für Telekommunikationsanschlüsse im Ausland vorgenommen werden. Bedingung ist jedoch, dass eine gezielte Erfassung von Anschlüssen deutscher Staatsangehöriger ausgeschlossen werden kann.[311]

Die meisten der dargestellten Methoden stehen allerdings nicht mehr exklusiv nur den Nachrichtendiensten zur Verfügung, sondern wurden schrittweise sowohl

---

[303] Vgl. *Grawe,* S. 124; *Rehbein,* S. 53. Zudem dürfen Brief- oder Postsendungen geöffnet und eingesehen werden. Als untechnische Maßnahmen fallen sie allerdings in die zweite Kategorie.

[304] Vgl. BT-Drs. 17/4278, S. 4.

[305] Vgl. *Droste,* Handbuch, S. 351, sowie BT-Drs. 14/5655, S. 13, 17. Um unverhältnismäßige Ausweitung zu verhindern, wird der Anteil der auf den Übertragungswegen zur Verfügung stehenden Übertragungskapazitäten nach § 10 IV 3, 4 G10 festgelegt. Bislang ist dieser Anteil auf maximal 20 % begrenzt.

[306] Die Rechtmäßigkeit dieser Norm wurde zuletzt durch BVerwG bestätigt, vgl. BVerwG NJW 2008, S. 2135, 2137.

[307] Vgl. Maunz/Dürig-*Durner,* Art. 10 Rn. 185.

[308] Vgl. *Hochreiter,* S. 26f, sowie BT-Drs. 14/5655, S. 18.

[309] § 5 II Nr. 1 G10.

[310] Vgl. *Grawe,* S. 124.

[311] Hierdurch sollen deutsche Staatsangehörige geschützt werden, vgl. BT-Drs. 14/5655, S. 20. Genau genommen geht es um Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind.

in die Strafprozessordnung als auch die Polizeigesetze aufgenommen.[312] Insbesondere durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15.7.1992 wurde das Befugnisarsenal der StPO um zahlreiche heimliche Ermittlungsmaßnahmen erweitert.[313] Im Laufe der Zeit wurden mit den §§ 98a, 99, 100a, 100c, 100f, 100h, 100i, 110a, 163d, 163e, 163f StPO nachträglich zahlreiche neue heimliche Ermittlungsbefugnisse eingeführt.[314] Aktuell werden etwa den Strafverfolgungsbehörden die inhaltliche Telekommunikationsüberwachung (§§ 100a, 100b StPO), die akustische Wohnraumüberwachung (§§ 100c, 100d, 100e), das Abhören des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen (§ 100f StPO), die Erhebung von Verkehrsdaten (§ 100g StPO), die Rasterfahndung (§ 98a StPO), der Einsatz von IMSI-Catchern (§ 100i StPO) sowie der Einsatz Verdeckter Ermittler (§ 110a I StPO) gestattet. Diese Befugnisse waren ursprünglich kein genuiner Bestandteil der Strafprozessordnung, weswegen die Anreicherung zum Teil als Recht der kleinen Buchstaben tituliert wird. Aktuell stehen der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten weitgehend identische Methoden zur Verfügung.[315]

Diese Parallelität widerspricht jedoch der ursprünglichen Intention des Trennungsgebots. Die darin angelegte Befugnistrennung ist nach überwiegender Ansicht nicht nur einseitig für die Nachrichtendienste vorgesehen, sondern gilt über den Wortlaut des Polizeibriefs hinaus auch in umgekehrter Richtung für die Polizei- und Strafverfolgungsbefugnisse. Den Polizei- und Strafverfolgungsbehörden sollte damit der Einsatz der typischen heimlichen, nachrichtendienstlichen Ermittlungsmethoden grundsätzlich nicht zustehen.[316] Zur Ermöglichung einer wirksamen Kontrolle staatlichen Handelns müsse die Polizei dem Bürger vielmehr mit „offenem Visier“ gegenübertreten.[317] Wie die Ausdehnung auf heimliche Ermittlungsbefugnisse verdeutlicht hat, wird diese Vorgabe vom Gesetzgeber nicht durchgehalten. Vielfach ist daher von einer „Vernachrichtendienstlichung“ der Polizei die Rede.[318]

Von dieser weitgehenden Parallelität gibt es nur vereinzelte Ausnahmen. Eine der wenigen den Diensten vorbehaltenen Befugnisse ist die optische Wohnraum-

---

312 Vgl. u.a. Borgs-Maciejewski/Ebert-*Borgs*, § 3 BVerfSchG Rn. 123; *Gröpl,* S. 312; *Nehm,* NJW 2004, S. 3293; *Singer,* OK, S. 293ff.

313 BGBl. I, S. 1302; vgl. *Hefendehl,* GA 2011, S. 211; *Hilger,* NStZ 1992, S. 460f.

314 Eine Aufzählung findet sich in § 101 I, IV StPO.

315 Vgl. *Gröpl,* S. 312.

316 Vgl. *Albert,* ZRP 1995, S. 107; *Baumann,* DVBl 2005, S. 800; *Droste,* Handbuch, S. 291; *Singer*, Die Kriminalpolizei 2006, S. 87. A.A. *Nehm,* NJW 2004, S. 3293.

317 Vgl. *Singer*, Die Kriminalpolizei 2006, S. 87.

318 So etwa *Baumann,* DVBl 2005, S. 800; *Singer*, Die Kriminalpolizei 2006, S. 87; *Wolff*, DöV 2009, S. 599.

überwachung. Während die strafverfahrensrechtliche Norm des § 100c StPO ausschließlich das Abhören und Aufzeichnen des gesprochenen Wortes ermöglicht, gestattet § 9 II 2 BVerfSchG zusätzlich die Anfertigung von Bildaufnahmen und Bildaufzeichnungen. Im Geheimdienstsektor ist damit neben der akustischen auch die optische Wohnraumüberwachung möglich.[319] Dieser Unterschied beruht indes nicht auf der Sicherheitsarchitektur, sondern folgt aus den verfassungsrechtlichen Vorgaben des Art. 13 III GG. Darin werden die zulässigen Eingriffe in die Unverletzlichkeit der Wohnung zu Strafverfolgungszwecken auf akustische Mittel begrenzt.[320]

Eine zweite Ausnahme bildet die strategische Überwachung der Telekommunikation nach §§ 1, 5 G10. Diese Erhebungsmethode ist trotz ihrer zum Teil irreführenden Bezeichnung als verdachtslose beziehungsweise strategische Rasterfahndung allein dem BND und damit dem Nachrichtendienstsektor vorbehalten.[321] Von der strafprozessualen Rasterfahndung nach § 98a StPO unterscheidet sie sich in mehrfacher Hinsicht. In beiden Fällen erfolgt zwar ein massenhafter Datenabgleich anhand bestimmter Merkmale, das heißt nach einem Raster,[322] die Recherche nach § 98a StPO erfolgt jedoch innerhalb eines bereits erhobenen Datenbestands öffentlicher beziehungsweise nichtöffentlicher Stellen. Demgegenüber werden bei der strategischen Kontrolle aktuelle Telekommunikationsvorgänge und damit noch nicht gespeicherte Inhalte gefiltert. Eine der strategischen Überwachung vergleichbare Befugnis steht den Strafverfolgungsbehörden nicht zur Verfügung.

Schließlich können flexibel neue Ermittlungsmethoden nach § 8 II 2 BVerfSchG in einer Dienstvorschrift benannt werden.[323] Die nachrichtendienstlichen Vorschriften enthalten insofern nur eine exemplarische Aufzählung der möglichen Ermittlungsmaßnahmen. Die Dienstvorschrift unterliegt als Verschlusssache der Geheimhaltung.[324] Aufgrund der Vorgaben des Gesetzesvorbehalts greifen diese neuen Befugnisse jedoch von vornherein nur bei weniger eingriffsintensiven Maßnahmen und sind vorliegend daher nicht von Interesse.[325]

Im Ergebnis finden sich in den geheimdienstlichen Ermächtigungsgrundlagen kaum Aufklärungsbefugnisse, die ausschließlich den Diensten zur Verfügung

---

[319] Auf diese Besonderheit verweisend *Hefendehl,* GA 2011, S. 211. Eine vergleichbare Ermächtigung findet sich auch in § 20 I Nr. 2 BKAG, der die Herstellung von Lichtbildern und Bildaufzeichnungen einer Person in oder aus Wohnungen gestattet.

[320] So Epping/Hillgruber-*Fink,* Art. 13 Rn. 15.

[321] Vgl. *Hefendehl,* GA 2011, S. 212.

[322] So Maunz/Dürig-*Durner,* Art. 10 Rn. 184.

[323] So *Rose-Stahl,* S. 70.

[324] So der Verweis bei *Rödder,* S. 90.

[325] Vgl. *Hefendehl,* GA 2011, S. 212.

Ermächtigungen	Nachrichtendienstsektor	Strafverfolgungssektor
Einsatz von VE/UCA	§§ 8 II, 9 I BVerfSchG	§§ 161, 163 StPO bzw. § 110a ff StPO
Akustische Wohnraumüberwachung	§§ 8 II, 9 II 1 BVerfSchG	§§ 100c, 100d StPO
Optische Wohnraumüberwachung	§§ 8 II, 9 II 2 BVerfSchG	–
Abfrage von Verkehrsdaten nach § 96 TKG	u.a. § 8a II Nr. 4, 5 BVerfSchG	§§ 100g, h StPO
Einsatz des IMSI-Catchers	u.a. § 9 IV BVerfSchG	§ 100i StPO
Zugriff auf Inhaltsdaten von Telekommunikationsvorgängen	Individualüberwachung nach §§ 1, 3 G10	§ 100a, b StPO
	Strategische Überwachung nach §§ 1, 5 G10	–

Tabelle 1

stehen.[326] Die im Geheimdienst- und Strafverfolgungssektor bestehenden Ermittlungsmethoden haben sich im Laufe der Jahre erheblich angenähert. Allerdings bleiben bestimmte Erhebungsmethoden, wie beispielsweise die optische Wohnraumüberwachung und die strategische Telekommunikationsüberwachung, den Nachrichtendiensten vorbehalten. Dies gilt auch für die heimliche Vorfeldaufklärung.[327] In den Besonderheiten geheimdienstlicher Ermittlungsbefugnisse wird damit nur ein beschränkter Einfluss der Sicherheitsarchitektur deutlich. Infolge der einseitigen Anwendung des Trennungsgebots heben sich die Dienste damit in methodischer Hinsicht weit weniger vom Strafverfolgungssektor ab als zunächst erwartet.

Die Tabelle 1 gibt einen Überblick über die unterschiedlichen Ermittlungsmethoden des Nachrichtendienst- und des Strafverfolgungssektors.

c) Zeitlicher Rahmen geheimdienstlicher Ermittlungen

Ausgehend von dem besonderen Beobachtungsauftrag der Geheimdienste orientieren sich geheimdienstliche Ermittlungen an spezifischen zeitlichen Rahmenbedingungen.

---

326 Vgl. u.a. *Gröpl,* S. 312f; *Gusy,* ZRP 2008, S. 37; *Hefendehl,* GA 2011, S. 211.

327 Vgl. *Weßlau,* S. 230.

aa) Beginn geheimdienstlicher Ermittlungen

Die nachrichtendienstlichen Ermittlungsschwellen sind in den Nachrichtendienstgesetzen und im Gesetz zu Art. 10 GG (G10) festgelegt. Ihre Besonderheiten werden bei einer Gegenüberstellung mit den Ermittlungsgrenzen der Strafverfolgungsbehörden deutlich. Aus diesem Grund beginnt die Darstellung mit den strafprozessualen beziehungsweise polizeilichen Grenzen. Anhand dieses Vergleichsmaßstabs werden im Anschluss die besonderen Rahmenbedingungen des geheimdienstlichen Kontexts verdeutlicht.

(1) Vergleichsmaßstab

Die Strafverfolgungs- und Polizeibehörden sind im Grundsatz an die Ermittlungsschwellen des Anfangsverdachts und der konkreten Gefahr gebunden.[328]

Im Bereich der Strafverfolgung ist die Grenze des Anfangsverdachts der Vorschrift des § 152 II StPO zu entnehmen.[329] Danach ist die Staatsanwaltschaft bei zureichenden tatsächlichen Anhaltspunkten verfolgbare Straftaten zum Einschreiten verpflichtet. Diese Verdachtsschwelle fordert über bloße Vermutungen hinausgehende konkrete Tatsachen, die nach allgemeiner kriminalistischer Erfahrung auf einen strafrechtlich relevanten Sachverhalt hindeuten.[330] Das Erreichen dieser Schwelle hat verschiedene rechtliche Konsequenzen. Auf einer ersten Ebene ist die Staatsanwaltschaft zur Erforschung des Sachverhalts sowie gegebenenfalls zur Einleitung und Durchführung des Ermittlungsverfahrens verpflichtet. Dieser Pflicht korrespondiert das Recht, entsprechende Nachforschungen durchzuführen.[331] Als dritte Konsequenz folgt aus dieser Rechten-Pflichten-Kombination im Umkehrschluss ein repressives Ermittlungsverbot.[332] Danach sind strafverfolgende Ermittlungen unterhalb der Schwelle des Anfangsverdachts grundsätzlich nicht gestattet.[333] Es gilt vielmehr eine „Redlichkeitsvermutung" gegenüber dem Bürger, dessen Freiheitsrechte nicht ohne Anlass beeinträchtigt werden sollen.[334] Gerade die mit einem Ermittlungsverfahren verbundenen Belastungen sind nach Ansicht des Gesetzgebers aus Gründen der Verhältnismäßigkeit nur bei Vorliegen eines

---

328 Vgl. etwa *Wolff,* S. 34.

329 Über § 163 StPO trifft diese Pflicht die Polizei in ihrer repressiven Funktion.

330 Vgl. BGH NStZ 1994, S. 499f; *Meyer-Goßner*, § 152 Rn. 4.

331 Vgl. *Hund,* ZRP 1991, S. 463; *Meyer-Goßner*, § 152 Rn. 3.

332 In diesem Sinne *Hund,* ZRP 1991, S. 463; *Roggan,* Polizeistaat, S. 39; *Rogall,* ZStW 103 (1991), S. 945; *Weßlau,* S. 279. Dieses Verbot ist nicht unumstritten, so Radtke/Hohmann-*Radtke,* § 152 Rn. 27 m.w.N.

333 So wohl im Ergebnis *Eisenberg/Conen,* NJW 1998, S. 2241; *Hund,* ZRP 1991, S. 463; *Keller/Griesbaum,* NStZ 1990, S. 418; *Roggan,* Polizeistaat, S. 39; *Weßlau,* S. 279.

334 Vgl. *Roggan,* Polizeistaat, S. 39; *Weßlau,* S. 337.

Anfangsverdachts gerechtfertigt.[335] Der Anfangsverdacht fungiert damit als Schnittstelle, an der sich das Verbot in die Berechtigung und Pflicht zu Durchführung repressiver Ermittlungsmaßnahmen wandelt.[336]

Im Vorfeld eines Anfangsverdachts sind lediglich sogenannten Vorermittlungen zulässig.[337] In diesem Stadium besteht eine Verdachtslage, die in ihrem Gewicht noch nicht zur Begründung eines Anfangsverdachts und damit zur Auslösung eines Ermittlungsverfahrens ausreicht.[338] Durch Vorermittlungsmaßnahmen werden lediglich bereits vorhandene Hinweise auf ihre Tauglichkeit zur Begründung eines Anfangsverdachts überprüft.[339] Solche Hinweise können beispielsweise aus einer Anzeige oder dem Vorliegen eines schädigenden Ereignisses resultieren. Die Vorermittlungen sollen dann das Bestehen einer *strafbaren* Handlung feststellen.[340] Vorermittlungen sind vor allem in Staatsschutz- und Terrorismusstrafsachen üblich, da die Begründung der generalbundesanwaltschaftlichen Sonderzuständigkeit oftmals eine besondere Verdachtsklärung der in § 120 I GVG genannten Delikte erfordert.[341] So ist beispielsweise der nach § 152 II StPO i.V.m. §§ 142a I, 120 GVG i.V.m. §§ 129, 129a StGB erforderliche Nachweis einer dauerhaften Vereinigung bei terroristischen Organisationen häufig wegen des Fehlens einer klaren Gruppenstruktur schwierig. Da Vorermittlungen in der StPO keine ausdrückliche Grundlage finden, sind sie auf einfache Erhebungsmaßnahmen beschränkt.[342] Zulässig wäre etwa die Einholung unverbindlicher Auskünfte oder die Gewinnung von Erkenntnissen aus allgemein zugänglichen Informationsquellen. Ein Rückgriff auf Ermächtigungsgrundlagen der Strafprozessordnung ist mangels Anfangsverdacht gerade nicht möglich.[343]

---

[335] In diesem Sinne *Eisenberg/Conen,* NJW 1998, S. 2241; *Forkert-Hosser,* S. 53f; *Hund,* ZRP 1991, S. 464; *Roggan,* Polizeistaat, S. 39; *Weßlau,* S. 337; *Wölfl,* JuS 2001, S. 479.

[336] *Eisenberg/Conen,* NJW 1998, S. 2241.

[337] Vgl. ausführlicher zur Thematik *Artzt,* S. 12ff; *Haas,* S. 24ff; *Lange,* S. 30ff; *Lange,* DRiZ 2002, S. 264ff; KK-*Pfeiffer/Hannich,* Einl. Rn. 33; *Rogall,* ZStW 103 (1991), S. 945.

[338] Vgl. *Meyer-Goßner*, § 152 Rn. 4a; Krekeler/Löffelmann-*Walther,* § 152 Rn. 6.

[339] Vgl. u.a. *Kramer,* Rn. 172; *Lange,* DRiZ 2002, S. 266; Krekeler/Löffelmann-*Walther,* § 152 Rn. 6.

[340] Vgl. *Wölfl,* JuS 2001, S. 479. Anders als das gesetzliche Ermittlungsverfahren werden diese Vorgänge nicht in das Js-Register nach § 47 AktO, sondern gemäß § 8 I 1 AktO zunächst in das AR-Register eingetragen, *Kramer,* Rn. 172; *Lange,* DRiZ 2002, S. 271. Verdichten sich die Hinweise zu einem Anfangsverdacht, erfolgt allerdings eine Umtragung in das Js-Register, vgl. *Pfeiffer* StPO, § 152 Rn. 1c.

[341] So *Diemer,* NStZ 2005, S. 666.

[342] Vgl. *Droste,* Handbuch, S. 297. Zur Diskussion hinsichtlich der tauglichen Rechtsgrundlage vgl. *Diemer,* NStZ 2005, S. 668.

[343] Vgl. u.a. Krekeler/Löffelmann-*Walther,* § 152 Rn. 6.

Diese im Grundsatz zulässigen Vorermittlungen sind von den im Strafverfahren unzulässigen Vor*feld*ermittlungen abzugrenzen. Bei Vorfeldermittlungen handelt es sich um Ermittlungen, die ohne konkreten Anlass oder Hinweis quasi ins Blaue hinein betrieben werden.[344] Dies beträfe etwa Fälle, in denen Ermittlungen allein aufgrund der bisherigen Erfahrung aufgenommen werden, dass es in einem bestimmten örtlichen Bereich häufiger zu Straftaten kommt als an einem anderen Ort.[345]

Einen zweiten Vergleichsmaßstab bilden die Ermittlungsschwellen aus dem Bereich der polizeilichen Gefahrenabwehr. Ein präventives Tätigwerden der Polizei ist nach den Landespolizeigesetzen in der Regel an das Vorliegen einer konkreten Gefahr gebunden.[346] Eine konkrete Gefahr fordert eine im Einzelfall bestehende Sachlage, die bei ungehindertem Ablauf mit hinreichender Wahrscheinlichkeit einen Schadenseintritt in sich birgt.[347] Dieser muss zeitlich unmittelbar bevorstehen.[348] Die Anforderungen an die Wahrscheinlichkeit des Schadenseintritts bestimmen sich in Abhängigkeit vom gefährdeten Rechtsgut. Das Ob und Wie der Gefahrenabwehr steht damit grundsätzlich im Ermessen der Polizei.[349]

(2) Ermittlungsschwellen der Geheimdienste

Im Gegensatz zu den Polizei- und Strafverfolgungsbehörden sind die Nachrichtendienste weder an die Grenze des Anfangsverdachts noch an eine konkrete Gefahrenschwelle gebunden. Der nachrichtendienstliche Beobachtungsauftrag orientiert sich vielmehr an den Vorgaben der §§ 8, 4 BVerfSchG, §§ 1, 2 BNDG und §§ 1, 3ff, 5ff G10. Diese stellen nach überwiegender Ansicht niedrigere Ermittlungsschwellen auf.[350] Nachfolgend werden die für die einzelnen Dienste maßgeblichen Ermittlungsschwellen getrennt dargestellt.

Dem BfV und dem MAD ist nach den §§ 8 I, 3, 4 I 3 BVerfSchG gegebenenfalls i.V.m. § 1 I 3 MADG die Erhebung der zur Aufgabenerfüllung „erforderlichen

---

344 Vgl. Krekeler/Löffelmann-*Walther,* § 152 Rn. 6; Radtke/Hohmann-*Radtke,* § 152 Rn. 28f; *Rogall,* ZStW 103 (1991), S. 945.

345 Vgl. zu dieser Unterscheidung Graf-*Beukelmann,* § 152 Rn. 6f, der auf die bestehende Verwertungsproblematik verweist.

346 Vgl. stellvertretend für viele *Gröpl,* S. 305.

347 Vgl. u.a. *Pieroth/Schlink/Kniesel,* § 5 Rn. 3.

348 Vgl. u.a. *Gröpl,* S. 306.

349 Vgl. u.a. *Pieroth/Schlink/Kniesel,* § 2 Rn. 8. Die Polizei unterliegt in ihrer präventiven Funktion insofern nicht dem Legalitäts-, sondern dem Opportunitätsprinzip. Wird die Polizei jedoch als Strafverfolgungsbehörde tätig, ist sie allein an die Vorgaben der Strafprozessordnung und damit das Legalitätsprinzip gebunden. Vgl. zur exklusiven Bindung der Polizeibeamten an die StPO im Bereich der Repression *Forkert-Hosser,* S. 32; KK-*Griesbaum,* § 161 Rn. 22.

350 Vgl. u.a. *Denninger,* KritV 1994, S. 236; *Droste,* Nachrichtendienste, S. 101; *Forkert-Hosser,* S. 66f; *Gusy,* KritV 1994, S. 243.

Informationen“ beim Vorliegen „tatsächlicher Anhaltspunkte“ für staatsgefährdende Bestrebungen oder Tätigkeiten gestattet.[351] Wesentliche zeitliche Schwelle ist damit das Vorliegen „tatsächlicher Anhaltspunkte“ i.S.d. § 4 I 3 BVerfSchG. Dieses Merkmal gilt selbst für den Einsatz nachrichtendienstlicher Mittel nach § 8 II StPO i.V.m. § 9 I BVerfSchG. Zwar fordert die Vorschrift des § 9 I BVerfSchG nach dem Wortlaut das Vorliegen von „Tatsachen“, die für den Eingriff zu erfüllenden Anforderungen an die Faktenlage werden dadurch allerdings nicht erhöht. Der Gesetzgeber wollte insofern keine unterschiedlichen Eingriffsschwellen schaffen.[352] Dieses Ergebnis wird durch die Einbeziehung der landesrechtlichen Verfassungsschutzregelungen bestätigt, welche sich trotz ähnlicher Abweichungen an der Grenze der §§ 3, 4 BVerfSchG orientieren. Anders als die Strafprozessordnung fordert das BVerfSchG damit keine „zureichenden tatsächlichen Anhaltspunkte“ für eine „Straftat“, sondern lediglich „tatsächliche Anhaltspunkte“ für „Bestrebungen“.[353] Der Großteil der Wissenschaft geht dementsprechend von einer im Vergleich zum Polizei- und Strafverfolgungssektor niedrigeren Ermittlungsschwelle aus.[354] Diese Besonderheit geheimdienstlicher Ermittlungen wird mit der thematischen Begrenzung auf bestimmte staatsschutzrelevante Bestrebungen begründet.[355]

Die angeführten sprachlichen Feinheiten führen faktisch allerdings nur in wenigen Grenzbereichen zu unterschiedlichen Ermittlungsgrenzen. So genügen für den strafprozessualen Anfangsverdacht bereits Indizien, für deren Richtigkeit nur eine gewisse Wahrscheinlichkeit sprechen muss.[356] Die für den Anfangsverdacht geforderte Tatsachenbasis ist damit bereits sehr niedrig angesetzt. Zwar ist damit weiterhin ein gewisser Verdacht notwendig, eine in der praktischen Anwendung sinnvolle

---

[351] Dies ergibt sich aus der genannten Verweisungskette. Insofern dürfen nach § 8 I BVerfSchG die zur Aufgabenerfüllung erforderlichen Informationen erhoben, verarbeitet und genutzt werden. Diese Erforderlichkeitsgrenze orientiert sich somit am Aufgabenbereich der Nachrichtendienste, welcher in § 3 BVerfSchG näher definiert ist und das Vorliegen bestimmter „Bestrebungen“ fordert. Der Begriff der Bestrebung wird in § 4 I BVerfSchG definiert; vgl. vertiefend *Droste,* Handbuch, S. 165f, 175.

[352] Vgl. dazu *Droste,* Handbuch, S. 305f, die von der „willkürlichen“ Wahl des einen oder anderen Begriffs spricht.

[353] Manche Landesverfassungsschutzgesetze fordern sogar nur das Vorliegen tatsächlicher Anhaltspunkte für den *Verdacht* einer Bestrebung. So z.B. § 3 I a.E. Verfassungsschutzgesetz Nordrhein-Westfalen (VSG NRW) oder § 5 Satz 1 LVerfSchG Rheinland-Pfalz.

[354] Vgl. hierzu u.a. *Forkert-Hosser,* S. 67; *Frister,* FS für Bemmann, S. 549; *Fromm,* in: Bundesamt für Verfassungsschutz, S. 55f; *Roggan,* Bürgerrechte & Polizei 2004, S. 37; *Roggan,* in: Roggan/Kutscha, S. 415; *Rose-Stahl,* S. 116; *Zöller,* JZ 2007, S. 765. Zur Notwendigkeit einer bestimmten Verdachtsschwelle *Ferse,* KritV 1994, S. 258; *Gusy,* StV 1995, S. 326.

[355] So u.a. *Forkert-Hosser,* S. 68; *Wolter,* Ehrengabe für Brauneck, S. 515.

[356] Vgl. *Hund,* ZRP 1991, S. 464; *Meyer-Goßner*, § 152 Rn. 4. Zur geringen Schwelle des Anfangsverdachts *Diemer,* NStZ 2005, S. 666.

Abstufung zu den tatsächlichen Anhaltspunkten des BVerfSchG erscheint jedoch schwierig.[357] In Bezug auf den Anfangsverdacht ist zudem zu berücksichtigen, dass die Anforderungen an den Verdachtsgrad mit steigender Wichtigkeit des Rechtsguts abnehmen.[358] Dieser Konnex führt gerade im Bereich terroristischer Straftaten zu einer Absenkung der Verdachtsanforderungen, da diese oftmals gegen den Staat beziehungsweise hochrangige Rechtsgüter gerichtet sind.[359] Die Unterscheidbarkeit vom Anfangsverdacht ist damit in der Praxis durchaus fraglich. Allerdings müssen die unterschiedlichen Bezugspunkte der jeweiligen Verdachtsschwellen in die Erwägungen mit einbezogen werden. Während sich strafrechtliche Ermittlungen auf strafbares beziehungsweise kriminelles Verhalten beziehen, genügt im Geheimdienstrecht das Vorliegen einer Bestrebung. Letztere erfordert weder rechtswidriges Vorgehen noch die Realisierung einer Gefahr.[360]

Damit ist der nachrichtendienstliche Anknüpfungspunkt weniger konkret als der im polizeilichen Gefahrenabwehrrecht. Die nachrichtendienstlichen Beobachtungen können sich auf abstrakte, weniger stark verdichtete Gefahrenlagen richten, wohingegen polizeiliche Maßnahmen in der Regel eine konkrete Gefahr erfordern.[361] In diesem Zusammenhang ist zudem eine seit 2002 bestehende Erweiterung in § 3 I Nr. 4 BVerfSchG zu berücksichtigen. Die Neuregelung dehnt den Beobachtungsauftrag auf Bestrebungen aus, die sich gegen den Gedanken der Völkerverständigung oder das friedliche Zusammenleben der Völker richten. Für diese Aufgabenzuweisung ist weder eine Schutzgutgefährdung noch eine Gewaltanwendung oder Vorbereitungshandlung erforderlich. Es ist vielmehr ausreichend, dass von den Bestrebungen „potentiell gefährdende Stimmungen" ausgehen, welche die Entstehung extremistischer Tendenzen begünstigen.[362] Damit werden vom Beobachtungsauftrag zum Teil bereits Verhaltensweisen erfasst, die sich im Bereich politischer Agitation abspielen. Eine vergleichbare Ermittlungsbefugnis steht den Strafverfolgungsbehörden nicht zur Verfügung.

Hierbei ist zu beachten, dass es sich bei diesen Ermittlungsschwellen lediglich um Minimalanforderungen handelt. Ebenso wie im Polizei- und Strafverfolgungssektor steigen mit zunehmender Eingriffsintensität die an die Ermittlungsschwelle zu stellenden Anforderungen. Ein Beispiel ist das Auskunftsersuchen nach § 8a BVerfSchG. Dieses erfordert das Vorliegen tatsächlicher Anhaltspunkte bezie-

---

357 Vgl. *Hund,* ZRP 1991, S. 464; *Keller/Griesbaum,* NStZ 1990, S. 416; *Lange,* DRiZ 2002, S. 266; *Wölfl,* JuS 2001, S. 479.

358 BVerfG NJW 2000, S. 55, 66.

359 So *Diemer,* NStZ 2005, S. 666.

360 Vgl. *Gröpl,* S. 307.

361 Stellvertretend für viele *Gröpl,* S. 307; *Hefendehl,* GA 2011, S. 213.

362 Kritisch zur Gesetzgebungskompetenz und Bestimmtheit der Neuregelung u.a. *Baldus,* ZRP 2002, S. 400; *Roggan,* in: Roggan/Kutscha, S. 440.

hungsweise Tatsachen für das Vorliegen schwerwiegender Gefahren für die in § 3 I BVerfSchG genannten Schutzgüter.[363]

Für den BND gelten ebenfalls abgesenkte Ermittlungsschwellen. Nach §§ 1 II, 2ff BNDG ist ihm das Sammeln von „erforderlichen Informationen einschließlich personenbezogender Daten" gestattet.[364] Anders als für Maßnahmen des BfV nach § 4 I 3 BVerfSchG fehlt in § 2 BNDG eine Bindung des BND an das Vorliegen tatsächlicher Anhaltspunkte. Erforderlich und ausreichend ist, dass sich die Informationserhebung thematisch im Rahmen seines Aufgabenspektrums bewegt und keine Regeln des Bundesdatenschutzgesetzes entgegenstehen.[365] Der BND muss kein bestimmtes oder gefährdendes Verhalten abwarten.[366] Dementsprechend kann er Beobachtungsmaßnahmen sogar noch früher einleiten als das BfV oder der MAD.[367] Lediglich die heimliche Informationsbeschaffung nach § 3 BNDG i.V.m. § 8 II BVerfSchG beziehungsweise die besonderen Auskunftsverlangen nach § 2a BNDG i.V.m. § 8a BVerfSchG verlangen eine tatsachengestützte Annahme.[368]

Weitere Besonderheiten gelten im Anwendungsbereich des G10. Dabei ist erneut zwischen der individuellen und der strategischen Kontrolle zu unterscheiden. Die individuelle Kontrolle nach §§ 1 I, 3 I G10 fordert „tatsächliche Anhaltspunkte für den Verdacht", dass jemand eine der genannten Katalogstraftaten „plant, begeht oder begangen hat". In der ersten Variante wird keine konkrete Vorbereitungshandlung gefordert, sondern das Vorliegen einer Planungsphase als ausreichend erachtet.[369] Im Extremfall kann die Individualkontrolle bereits dazu genutzt werden, den Verdächtigen überhaupt zu identifizieren. Liegen beispielsweise tatsächliche Hinweise dafür vor, dass sich der Verdächtige in einem bestimmen Gebäude aufhält, so gestattet dieser Verdacht die eingrenzende Individualkontrolle gegen alle Bewohner.[370] Die zulässige Anknüpfung an die Planungsphase erweist sich als zentraler Unterschied zum Strafrecht, das von einer strafrechtlichen Relevanz erst ab einer

---

363 Vgl. hierzu BT-Drs. 17/6925, S. 12.

364 Anders als bei den anderen Nachrichtendienstgesetzen werden im BNDG die Erhebungsbefugnisse nicht bereits in der Aufgabenbeschreibung des § 1 II 1 BNDG, sondern erst im Rahmen der Befugnisnorm des § 2 I BNDG festlegt; vgl. *Wolff,* S. 90.

365 Vgl. § 2 I 2. Halbsatz BNDG.

366 Vgl. *Wolff,* S. 90.

367 Vgl. *Forkert-Hosser,* S. 68.

368 Vgl. *Forkert-Hosser,* S. 67.

369 Nach *Droste,* Handbuch, S. 339, ist aber zumindest ein „nach außen wie auch immer in Erscheinung getretenes systematisches Handlungskonzept" erforderlich.

370 Manche Autoren vergleichen diese Überwachungsmaßnahme mit der Suche der Nadel im Heuhaufen. Diese Suche kann mit Hilfe der Individualkontrolle durchgeführt werden, wenn ausreichend Hinweise darauf bestehen, dass sich die Nadel tatsächlich im Heuhaufen befindet, nicht dagegen „um festzustellen, ob sie sich darin befindet", so Borgs-Maciejewski/Ebert-*Borgs*, § 2 G10 Rn. 9.

Vorbereitungshandlung i.S.d. § 30 StGB ausgeht.[371] Die Planungsphase ist für das Strafrecht demgegenüber nicht von Interesse.[372] Zieht man vergleichend zusätzlich die parallele strafprozessuale Befugnis in § 100a StPO heran, so werden die Unterschiede noch deutlicher. So fordert § 100a StPO „bestimmte Tatsachen" für den Verdacht einer schweren Katalogtat. Diese „bestimmten Tatsachen" sind deutlich substantiierter darzulegen als bloße „tatsächliche Anhaltspunkte". Die Individualkontrolle nach dem G10 ist damit zu einem früheren Zeitpunkt möglich als die strafprozessuale Telekommunikationsüberwachung.[373] Etwas anders gilt nach § 3 II 2 G10 lediglich dann, wenn der Verdächtige sicher feststeht. In diesem Fall darf die Individualkontrolle gegen andere Personen nur bei Vorliegen bestimmter Tatsachen durchgeführt werden. Diese Schwelle ist derjenigen des § 100a III StPO sehr ähnlich.[374]

Die für die strategische Telekommunikationsüberwachung maßgebliche Ermittlungsschwelle ergibt sich aus § 5 I 1, 3 Nr. 2 G 10. Danach dürfen Informationen gesammelt werden, deren Kenntnis „notwendig" ist, um bestimmte aufgezählte Großgefahren „rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen". Diese Gefahren betreffen unter anderem Gefährdungen durch bewaffnete Angriffe, die Begehung internationaler terroristischer Anschläge, die Verbreitung von Kriegswaffen oder der Betäubungsmittelhandel.[375] Die Kontrolle konkreter Einzelpersonen ist gerade nicht beabsichtigt, sodass das Vorliegen eines der Strafprozessordnung vergleichbaren tatbezogenen Verdachts nicht erforderlich ist.[376] Eine Konkretisierung der Gefahr oder eines Verdachts muss nicht abgewartet werden. Nach Ansicht des Bundesverfassungsgerichts reicht es vielmehr aus, dass „bei Durchführung der Überwachungsmaßnahme Erkenntnisse über bestehende Gefahrenlagen […] zu erwarten sind".[377] Die strategische Telekommunikationsüberwachung gestattet damit eine anlassunabhängige, sachbezogene Überwachung.[378]

---

371 Vgl. *Griesbaum,* FS für Nehm, S. 133. Diese Schwelle ist mit den zwei weiteren Tatbestandsalternativen „begeht oder begangen hat" jedoch zweifelsohne erfüllt.

372 So Borgs-Maciejewski/Ebert-*Borgs*, § 2 G10 Rn. 12; *Droste,* Handbuch, S. 339, 345.

373 Vgl. *Wolff,* DöV 2009, S. 604f. Zudem müssen für eine Anwendung der parallelen StPO-Norm die zusätzlichen Voraussetzungen von § 100a I Nr. 1–3 StPO erfüllt sein. Borgs-Maciejewski/Ebert-*Borgs*, § 2 G10 Rn. 6, 8, verweist darauf, dass der Rechtsausschuss diese Unterscheidung bewusst getroffen hat, um die Möglichkeiten einer effektiven und frühzeitigen Gefahrenabwehr nicht unnötig zu behindern.

374 Vgl. Borgs-Maciejewski/Ebert-*Borgs*, § 2 G10 Rn. 12.

375 § 5 I G10.

376 Vgl. *Grawe,* S. 124. So genügten bereits Informationen, die auf die Existenz von Schläfern im Umkreis des Überwachten hinwiesen, vgl. BVerwG NJW 2008, S. 2135, 2137. Allerdings ist zu berücksichtigen, dass die vorliegenden Ausführungen nur die zeitlichen Ermittlungsschwellen betreffen. Im Übrigen ist die strategische Überwachung an relativ strikte Voraussetzungen gebunden, vgl. hierzu unter Teil 2, III.B.1.e)aa).

377 BVerwG NJW 2008, S. 2135, 2137.

378 Vgl. Borgs-Maciejewski/Ebert-*Borgs*, § 3 G10 Rn. 2; *Hellmann,* S. 125; *Riegel,* ZRP 1995, S. 176; *Roggan,* in: Roggan/Kutscha, S. 427.

Damit sind die Eingriffsschwellen im Bereich der strategischen Telekommunikationsüberwachung erneut deutlich abgesenkt. Im Grundsatz können die Nachrichtendienste mit ihren Beobachtungsmaßnahmen überwiegend früher beginnen als die Polizei oder die Strafverfolgungsbehörden.[379]

(3) Annäherungstendenzen

Die klassische Abgrenzung der nachrichtendienstlichen Ermittlungsschwellen zur polizeilichen Gefahr und zum strafprozessualen Anfangsverdacht wird in den rechtlichen Reaktionen auf neue Formen der Kriminalität zunehmend verwässert.[380] Sowohl auf materiell-rechtlicher als auch auf prozessualer Seite erfolgt eine Annäherung. Materiell-rechtlich wird der strafrechtliche Schutz unter anderem durch die Vorverlagerung der Strafbarkeit ausgeweitet.[381] Durch die Schaffung neuer abstrakter Gefährdungs- und Organisationsdelikte sowie die zunehmende Kriminalisierung von Vorbereitungshandlungen werden die zeitlichen Rahmenbedingungen weiter gelockert.[382] Insbesondere im Bereich der OK und des internationalen Terrorismus kommt es zunehmend zu einer Überschneidung strafrechtlicher und nachrichtendienstlicher Tätigkeitsfelder.[383]

Auf prozessualer Seite lässt sich eine schrittweise Entkoppelung des Polizei- und Strafrechts von klassischen Gefahren- und Verdachtsschwellen beobachten.[384] Mit der sogenannten vorbeugenden Bekämpfung von Straftaten, der Strafverfolgungsvorsorge und den Vorermittlungsverfahren bestehen bereits heute Ermittlungsmöglichkeiten, die nicht an den klassischen Anfangsverdacht gebunden sind.[385] Im Polizeirecht sind die Ausnahmen von der klassischen Gefahrenschwelle mit der sogenannten Gefahrerforschung,[386] der Gefahrenvorsorge,[387] der Vorsorge für die

---

[379] So u.a. *Fromm,* in: Bundesamt für Verfassungsschutz, S. 55f. Dies gilt selbst für das präventiv-polizeiliche Gefahrenabwehrrecht. Dieses ist zwar anders als das Strafverfolgungsrecht nicht vergangenheitsbezogen, dennoch geht es um eine ereignisbezogene Reaktion auf eine bestehende Gefahrenlage, vgl. *Roggan,* Polizeistaat, S. 33.

[380] Vgl. zu dieser Tendenz *Kornblum,* S. 55; KK-*Pfeiffer/Hannich,* Einl. Rn. 22b.

[381] Vgl. *Hund,* ZRP 1991, S. 464; *Zöller,* Terrorismusstrafrecht, S. 501. Vertiefend *Sieber,* NStZ 2009, S. 353ff; *Zöller,* Terrorismusstrafrecht, S. 588.

[382] So etwa in den §§ 129, 129a StGB; vgl. hierzu insgesamt *Hefendehl,* GA 2011, S. 216; *Forkert-Hosser,* S. 49, 86ff; *Rehbein,* S. 91.

[383] So u.a. *Droste,* Nachrichtendienste, S. 300f.

[384] Vgl. hierzu *Hefendehl,* GA 2011, S. 209.

[385] Eine kurze Übersicht findet sich bei *Wolter,* Ehrengabe für Brauneck, S. 515f.

[386] Bei der Gefahrerforschung handelt es sich um die polizeirechtliche Entsprechung der Verdachtserforschung im Rahmen der Vorermittlungen, vgl. *Rogall,* ZStW 103 (1991), S. 945. Grundrechtseingriffe werden in diesem Stadium wohl nicht gestattet; vgl. vertiefend bei *Forkert-Hosser,* S. 86ff, 91.

[387] Die Gefahrenvorsorge erfasst Maßnahmen, welche die Entstehung künftiger Gefahren verhüten soll, vgl. *Forkert-Hosser,* S. 92 m.w.N. und Beispielen.

künftige Gefahrenabwehr[388] und der vorbeugenden Bekämpfung von Straftaten[389] sogar noch zahlreicher. Im gesamten Sicherheitswesen wird damit eine Ausweitung auf den Vorfeldbereich deutlich.[390]

Trotz der beschriebenen Annäherungstendenzen sind weiterhin gewisse verallgemeinerungsfähige Unterschiede feststellbar. Die Minimalanforderungen an die Verdachtsschwellen weichen zumindest im Anwendungsbereich des BNDG und des G10 weiterhin von denen des Strafverfolgungssektors ab.[391] Den Diensten ist damit ein Beobachtungsfeld zugänglich, das den Strafverfolgungsbehörden bislang noch nicht offen steht. Verdachts- und anlasslose Ermittlungen etwa sind nach der Strafprozessordnung weiterhin unzulässig.[392] Zudem bleiben flächendeckende Beobachtungsmaßnahmen weiterhin den Nachrichtendiensten vorbehalten.[393] Diese Unterschiede rechtfertigen sich vor dem Hintergrund der Funktion der Dienste als Frühwarnsystem zum Schutz von Rechtsgütern überragender Bedeutung.[394] Zur Erfüllung dieses Auftrags müssen sie in einem (noch) nicht strafbewehrten Vorfeld beobachtend tätig werden dürfen.[395] Es bleibt abzuwarten, wie lange diese Annahmen gültig sind. Erste Anhaltspunkte für eine Änderung bietet das Urteil des Bundesverfassungsgerichts vom 2. März 2010 zur Vorratsdatenspeicherung.[396] Darin erklärte das Gericht zwar die anlasslose Vorratsdatenspeicherung für verfassungswidrig,[397] gleichzeitig betonte es jedoch, dass eine vorsorgliche anlasslose Speiche-

---

388 Erfasst sind dauerhafte, vorbereitende Maßnahmen zur Verhinderung künftiger Gefahren durch eine vorsorgliche Informationserfassung; vgl. *Forkert-Hosser,* S. 93ff.

389 Die vorbeugende Bekämpfung von Straftaten nach den Polizeigesetzen gliedert sich nach ü.A. in die „Verhütung von Straftaten" und die „Vorsorge für die künftige Strafverfolgung"; vgl. *Kistner-Bahr*, S. 112f. Die Straftatverhütung soll die Verwirklichung von Straftatbeständen verhindern. Bei der Strafverfolgungsvorsorge werden die Daten zwar im Vorfeld erhoben, sollen aber in einem künftigen Strafverfahren bereitgestellt werden. Die Maßnahme weist damit tendenziell eine repressive Zielsetzung auf. Die Verortung im Polizeirecht wird von der Rechtsprechung zwar bislang gestattet, überwiegend jedoch als Fremdkörper empfunden; vgl. *Forkert-Hosser,* S. 40f m.w.N.

390 Vgl. zu dieser Entwicklung *Gröpl,* S. 308; *Hefendehl,* GA 2011, S. 214f; *Kornblum,* S. 53f; *Zöller,* Terrorismusstrafrecht*,* S. 501f.

391 Demgegenüber sind die theoretisch abgesenkten Ermittlungsschwellen nach dem BVerfSchG und dem MADG in praktischer Hinsicht weniger relevant.

392 Vgl. *Meyer-Goßner*, § 152 Rn. 4a; Radtke/Hohmann-*Radtke,* § 152 Rn. 28.

393 So *Rehbein,* S. 92.

394 So u.a. *Forkert-Hosser,* S. 68. Nach ihr obliegt den Nachrichtendiensten die „Wahrung der staatlichen Integrität, der Erhalt der Demokratie und damit die Aufrechterhaltung der grundlegenden Voraussetzungen des Gemeinwesens".

395 Dementsprechend versteht auch das PKGr die Post- und Fernmeldekontrolle durch die Nachrichtendienste als eine „Erkundung im strafrechtlichen Vorfeld", vgl. den Bericht des PKGr vom 4.3.2004 in BT-Drs. 16/2616, S. 4.

396 Vgl. zu dieser Einschätzung *Beukelmann,* NJW-Spezial 2010, 184; *Forkert-Hosser,* S. 114f.

397 Vgl. BVerfG MMR 2010, S. 356ff, bzw. BVerfG NJW 2010, S. 833ff, zu den §§ 113a, 113b TKG, 100g StPO.

rung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung mit Art. 10 GG „nicht schlechthin unvereinbar" sei, wenn der Eingriff einem legitimen Gemeinwohlzweck dient und im Übrigen verhältnismäßig ist.[398]

bb) Ende geheimdienstlicher Ermittlungen

Weitere Besonderheiten ergeben sich in Bezug auf den Abschlusszeitpunkt geheimdienstlicher Ermittlungen. Die Dienste unterliegen entsprechend ihrem langfristig angelegten Beobachtungsauftrag dem Opportunitätsprinzip. Danach sind sie ab Überschreiten bestimmter Ermittlungsschwellen zwar zur Beobachtung,[399] nicht aber zur Weiterleitung gesammelter Informationen an die Strafverfolgungsbehörden oder die Gerichte verpflichtet. Der Handlungsspielraum der Dienste weicht damit erheblich von dem der Strafverfolgungsbehörden ab, welche als Folge des Legalitätsprinzips spätestens ab Bestehen eines hinreichenden Tatverdachts i.S.d. § 170 I StPO zur Einreichung einer Anklageschrift verpflichtet sind.[400] Der in Strafverfolgungsfragen maßgebliche Gleichbehandlungs- und Gerechtigkeitsgedanke würde ins Leere laufen, wenn die Strafverfolgungsbehörden zwar zu Ermittlungen verpflichtet wären, später jedoch von einer Anklageerhebung absehen könnten. Während die Strafverfolgungsbehörden ab dem genannten Zeitpunkt die Verfahrensherrschaft grundsätzlich an das Gericht abgeben, wird der Beobachtungsauftrag der Dienste nicht ohne Weiteres durch das Erreichen einer bestimmten Verdachtsschwelle beendet. Da die Dienste prinzipiell nicht die Strafverfolgung einzelner Täter, sondern die Erlangung von Hintergrund- und Strukturwissen bezwecken, können sie ihre Beobachtungen bei Bestehen eines hinreichenden Tatverdachts grundsätzlich fortführen.[401]

Die Notwendigkeit einer solchen ungehinderten Strukturaufklärung ist vor allem bei der Terrorismusbekämpfung offensichtlich. In diesem Bereich wird der Zugang zu Informationen durch die Existenz komplexer, internationaler und zersplitterter Strukturen sowie die sprachliche und kulturelle Abschottung erheblich erschwert.[402] Der Zugang zu Insiderinformationen wäre kaum möglich, wenn jeder Tatverdacht eine öffentliche Anklageerhebung und damit die Enttarnung der Ge-

---

[398] So BVerfG MMR 2010, S. 356, 359, bzw. BVerfG NJW 2010, S. 833, 838 Abschnitt 207.

[399] Vgl. *Droste,* Handbuch, S. 199.

[400] In diesem Fall sind die Ermittlungsergebnisse nach § 199 II 2 StPO vollständig an das Gericht zu übersenden; vgl. insgesamt *Roxin/Schünemann,* S. 296 Rn. 10f; KK-*Schmid,* § 170 Rn. 10; *Strauß,* NStZ 2006, S. 559; vgl. SK-StPO-*Wohlers,* § 170 Rn. 2, 36. Vor diesem Zeitpunkt ist den Strafverfolgungsbehörden eine Verzögerung aus kriminaltaktischen Gründen ebenfalls gestattet, vgl. *Gärditz,* § 152 Rn. 9.

[401] Vgl. u.a. *Albert,* in: Korte/Zoller, S. 98f; *Frister,* FS für Bemmann, S. 551; *Fromm,* in: Bundesamt für Verfassungsschutz, S. 56; *Korte,* in: Korte/Zoller, S. 53ff; *Kuhlmann,* in: Korte, S. 154; *Rödder,* S. 109.

[402] Vgl. *Gröpl,* S. 307; *Korte,* in: Korte/Zoller, S. 61; *Wache,* Terrorismus, S. 147f.

heimdienste zur Folge hätte.[403] Dementsprechend dürfen die Dienste ihre Aufklärungsmaßnahmen selbst dann fortsetzen, wenn genügend Informationen für die Einleitung eines Strafverfahrens vorliegen.[404] Ihnen wird in dieser Hinsicht ein gewisser Ermessensspielraum zugestanden.[405] Bei besonders schwerwiegenden Straftaten relativieren sich diese Unterschiede jedoch. Liegt beispielsweise eine Katalogstraftat nach § 138 StGB vor, so kann sich der bestehende Ermessensspielraum zu einer Übermittlungspflicht verdichten, die die nachrichtendienstlichen Belange zurücktreten lässt.[406]

cc) Zwischenergebnis zu zeitlichen Rahmenbedingungen

Die deutschen Nachrichtendienste können frühzeitig, umfassend und langfristig Informationen erheben. Dieser im Vergleich zu anderen Sicherheitsbehörden umfassendere zeitliche Aktionsradius rechtfertigt sich angesichts der zu schützenden, hochrangigen Rechtsgüter.[407] Im Bereich der schweren Kriminalität verlieren die beschriebenen Unterschiede allerdings an Relevanz.

d) Durchsetzungsmöglichkeiten

Ein weiteres Merkmal geheimdienstlicher Ermittlungsbefugnisse geht auf die befugnisrechtliche Dimension des Trennungsgebots zurück. Danach dürfen den Diensten ausdrücklich keine „polizeilichen Befugnisse“ zur Verfügung stehen. Ihnen ist jede Art von Maßnahme mit Gebots-, Verbots- oder Duldungscharakter untersagt, sodass sie im Rahmen ihres Beobachtungsauftrags letztlich um die Handlungs- und Sanktionskomponente beschnitten sind.[408] Folglich dürfen sie weder Durchsuchungen, Beschlagnahmen, Identitätsfeststellungen, Festnahmen oder körperliche Untersuchungen selbst durchführen noch um entsprechende Befugnisse im Wege der Amtshilfe ersuchen.[409] Einfachgesetzlich ist dies in § 8 III 1. Halbsatz BVerfSchG, § 2 III 1 BNDG sowie § 4 II 1. Halbsatz MADG verankert. Erst diese

---

403 Vgl. u.a. *Kuhlmann,* in: Korte, S. 154.

404 Vertiefend zu diesem Opportunitätsprinzip *Droste,* Nachrichtendienste, S. 102; *Korte,* in: Korte/Zoller, S. 53ff; *Zöller,* in: Roggan/Kutscha, S. 500. Vgl. Borgs-Maciejewski/Ebert-*Borgs*, § 1 G10 Rn. 5, für Maßnahmen nach dem G10.

405 So *Rödder,* S. 110; *Zöller,* in: Roggan/Kutscha, S. 500.

406 Vgl. Borgs-Maciejewski/Ebert-*Borgs*, § 3 BVerfSchG Rn. 38, § 1 G10 Rn. 5; *Korte,* in: Korte/Zoller, S. 53ff; *Rödder,* S. 110; *Schäfer/Wache/Meiborg*, Rn. 349; *Zöller,* in: Roggan/Kutscha, S. 500.

407 So *Droste,* Nachrichtendienste, S. 101.

408 Vgl. *Droste,* Handbuch, S. 223, 294; *Ferse,* KritV 1994, S. 260; *Singer,* OK, S. 61; *Soiné,* NStZ 2007, S. 247f; kritisch *Kutscha,* NVwZ 2013, S. 324.

409 Vgl. BVerfG, NJW 2011, S. 2417, 2420; *Kutscha,* NVwZ 2013, S. 324.

Begrenzung rechtfertigt nach Ansicht des Gesetzgebers die Konzeption der Dienste als Frühwarnsystem und damit die relativ niedrigen Eingriffsschwellen.[410]

Diese Vorgabe wurde vonseiten der Nachrichtendienste bislang strikt eingehalten. Bezieht man die zunehmende Ergänzung des Strafverfahrens- und Polizeirechts, um nachrichtendienstliche Methoden mit ein, so entsteht der Eindruck, dass die deutschen Dienste im Verhältnis zur Polizei und den Strafverfolgungsbehörden in ihren rechtlichen Möglichkeiten schwächer aufgestellt sind.[411] Allerdings können Polizei- und Strafverfolgungsbehörden die einzelnen Zwangsbefugnisse ebenso wenig uneingeschränkt einsetzen. Diese sind in der Regel an strenge Voraussetzungen und das Vorliegen einer ausreichenden Tatsachenbasis gebunden. Ein Einsatz im Vorfeldbereich ist grundsätzlich unzulässig. Zudem verfügen die deutschen Nachrichtendienste mit der optischen Wohnraumüberwachung und der strategischen Telekommunikationsüberwachung weiterhin über exklusive Erhebungsbefugnisse. Schließlich führt die Annäherung an das nachrichtendienstliche Befugnisarsenal nicht zwingend zu einer Parallelität der Informationserhebung selbst. Das Stichwort der Vergeheimdienstlichung der sonstigen Sicherheitsbehörden erstreckt sich lediglich auf die Erweiterungen der verfügbaren Ermittlungsmethoden, nicht jedoch die jeweils geltenden Anordnungsvoraussetzungen und Grenzen.[412] Inwieweit sich die Erhebungsvoraussetzungen der Dienste von denen anderer Sicherheitsbehörden absetzen, ist Gegenstand des nächsten Abschnitts.

e) Ausgewählter Vergleich der Erhebungsvoraussetzungen

Nach Darstellung der unterschiedlichen Ermittlungsschwellen und Durchsetzungsmöglichkeiten werden nachfolgend die materiellen Voraussetzungen der nachrichtendienstlichen Informationserhebung einer generellen Betrachtung unterzogen. Die in diesem Zusammenhang feststellbaren Besonderheiten bilden einen wesentlichen Anknüpfungspunkt für die Sonderbehandlung im Rahmen der Beweisverwertung. Die allgemeinen Charakteristika werden zunächst für generelle Erhebungsvoraussetzungen sowie speziell bezogen auf einzelne Ermittlungsmethoden herausgearbeitet.

aa) Allgemeine Anforderungen

In den Nachrichtendienstgesetzen finden sich einige Vorgaben, die bei sämtlichen Ermittlungsmaßnahmen zu beachten sind. Nach § 8 I, V BVerfSchG müssen die Maßnahmen etwa dem Grundsatz der Erforderlichkeit beziehungsweise Verhältnismäßigkeit genügen. Nach § 9 I 2 BVerfSchG sind Informationen vorrangig

---

410 So *Forster*, in: Polizei-Führungsakademie Münster, S. 325.

411 Vgl. *Hefendehl,* GA 2011, S. 211.

412 Zu diesem Aspekt der Vergeheimdienstlichung vgl. *Hefendehl,* GA 2011, S. 209.

aus allgemein zugänglichen Quellen zu gewinnen.[413] Oftmals handelt es sich bei diesen Vorgaben nicht um eigenständige Anforderungen, sondern um bloße Wiederholungen allgemeiner Verhältnismäßigkeits- beziehungsweise Subsidiaritätserwägungen. Sie sind relativ abstrakt beziehungsweise allgemein formuliert und damit oftmals unpräziser als vergleichbare Strafprozessnormen.[414]

Im Übrigen muss zwischen den einzelnen Erhebungsmethoden differenziert werden. Für den Bereich der schlichten Erhebungsmaßnahmen nach § 8 I BVerfSchG sind aufgrund der geringen Eingriffsintensität keine weiteren Voraussetzungen zu erfüllen.[415] Eine Begrenzung erfolgt lediglich durch den Grundsatz der Erforderlichkeit.[416] Bei Befragungen ist der Betroffene zudem vorab auf die Freiwilligkeit eventueller Aussagen hinzuweisen.[417] Da sie die Grundrechte nicht weiter berühren, sind diese Erhebungsmethoden für die vorliegende Untersuchung nicht weiter von Relevanz. Mit steigender Eingriffsintensität steigen allerdings auch die im Geheimdienstsektor an die Informationserhebung zu stellenden Anforderungen.[418]

bb) Einsatz Verdeckter Ermittler

Von weit größerer Bedeutung ist der Einsatz nachrichtendienstlicher Mittel nach §§ 8 II, 9 BVerfSchG. Zu diesen zählt unter anderem der sogenannte *Undercover Agent* (UCA). Dieser wird in den Vorschriften zwar nicht ausdrücklich genannt, ist als nachrichtendienstliches Mittel jedoch allgemein anerkannt.[419] Beim UCA handelt es sich um einen Bediensteten der Nachrichtendienste, der unter einer Legende ermittelnd tätig wird. Sein Einsatz ist abgesehen vom Vorliegen tatsächlicher Anhaltspunkte und einer behördeninternen Genehmigung an keine weiteren Voraussetzungen gebunden.[420] Der im Strafverfahrensrecht damit vergleichbare Einsatz

---

413 Vgl. *Droste,* Handbuch, S. 225.

414 Vgl. *Hefendehl,* GA 2011, S. 213, 215. Allerdings spielen diese Klauseln auch im Rahmen der StPO keine allzu große Bedeutung.

415 Vgl. *Droste,* Handbuch, S. 229. Die parallele Befugnis für die Strafverfolgungsbehörden ist in § 161 I 1 StPO, vgl. BT-Drs. 14/1484, S. 23, geregelt.

416 Vgl. BT-Drs. 14/1484, S. 23, ebenso Graf-*Patzak,* § 161 Rn. 4.

417 § 8 IV 2 BVerfSchG.

418 Ein besonderes Auskunftsverlangen nach § 8a BVerfSchG fordert beispielsweise „schwerwiegende Gefahren" für nachrichtendienstliche Schutzgüter des § 3 I BVerfSchG. In § 8a III BVerfSchG wird zudem der Kreis der tauglichen Auskunftspflichtigen eingegrenzt. Im Vergleich zu schlichten Erhebungsmaßnahmen sind diese höher angesetzt, allerdings nur unwesentlich. Durch das Erfordernis einer qualifizierten Gefahr werden zwar sprachlich die Erhebungsvoraussetzungen erhöht, bei genauerer Betrachtung führt das Gefahrelement indes zu keinem tatsächlichen Bestimmtheitsgewinn. Es eröffnet vielmehr einen erheblichen Beurteilungsspielraum, der die Letztentscheidungsbefugnis bei den Geheimdiensten belässt; vgl. *Hefendehl,* GA 2011, S. 213.

419 Vgl. *Rehbein,* S. 40.

420 Vgl. *Droste,* Handbuch, S. 278; *Droste,* Nachrichtendienste, S. 113; *Rehbein,* S. 40.

eines Verdeckten Ermittlers (VE) unterliegt demgegenüber deutlich höheren Anforderungen. Die Parallelvorschriften der §§ 110a, 110b StPO fordern einen Anfangsverdacht, der sich auf Straftaten von erheblicher Bedeutung beziehen muss. Diese Straftat muss entweder einem explizit genannten Kriminalitätsbereich angehören, durch eine besonders gefährliche Begehungsweise gekennzeichnet sein oder als Verbrechen der Wiederholungsgefahr unterliegen.[421] Darüber hinaus ist nach § 110b StPO die Zustimmung der Staatsanwaltschaft nach Abs. 1 beziehungsweise bei einem qualifizierten Einsatz nach Abs. 2 die Zustimmung eines Richters erforderlich.[422] Der strafprozessuale VE ist zudem an einen expliziten Ermittlungsauftrag gebunden, während der UCA langfristige Strukturaufklärung betreiben darf.[423] Die Anordnungsvoraussetzungen im Geheimdienstsektor sind damit sowohl in materieller als auch formeller Hinsicht geringer angesetzt als bei vergleichbaren Maßnahmen im Strafverfahrensrecht. Diese Erkenntnis ist auf den Einsatz nachrichtendienstlicher V-Männer oder Informanten übertragbar, welcher in der Regel nur dem Verhältnismäßigkeitsgrundsatz des § 9 I BVerfSchG unterliegt.

cc) Wohnraumüberwachung

Deutlich strengeren Bedingungen unterliegt die Wohnraumüberwachung nach § 9 II BVerfSchG. Aufgrund des Eingriffs in Rechte nach Art. 13 GG ist die Überwachung an das Vorliegen einer gegenwärtigen gemeinen Gefahr beziehungsweise Lebensgefahr, die Beachtung des Verhältnismäßigkeitsgrundsatzes und die Aussichtslosigkeit polizeilicher Hilfe gebunden. Anders als nach den §§ 100c, 100d StPO muss die Gefahr nicht näher spezifiziert werden. Die nachrichtendienstlichen Voraussetzungen sind dennoch vergleichsweise streng, sodass manche Autoren von einem faktischen Verbot der optischen Wohnraumüberwachung ausgehen.[424]

dd) Telekommunikationsüberwachung

Im Bereich der Telekommunikationsüberwachung sind die Voraussetzungen nach dem G10 zu beachten.[425] Die Individualkontrolle richtet sich nach §§ 1, 3 G10. Diese knüpfen die Überwachung an das Vorliegen einer der dort aufge-

---

421 Der Gesetzestext nennt u.a. Delikte auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs sowie Staatsschutzdelikte oder gewerbs- oder bandenmäßig organisierte Delikte; vgl. auch *Zöller,* StraFo 2008, S. 19.

422 Vgl. *Droste,* Nachrichtendienste, S. 112. Qualifiziert ist der Einsatz gegen einen bestimmten Beschuldigten oder bei Betreten einer Wohnung.

423 Vgl. *Droste,* Handbuch, S. 277; *Droste,* Nachrichtendienste, S. 112.

424 So u.a. *Droste,* Handbuch, S. 316; *Rehbein,* S. 48. Erforderlich sind u.a. Straftaten von erheblicher Bedeutung aus bestimmten Kriminalitätsbereichen sowie eine Schwere im Einzelfall.

425 Die ebenfalls gestatteten Eingriffe in das Brief- und Postgeheimnis bleiben vorliegend aus Gründen der Übersichtlichkeit außer Betracht.

zählten Katalogstraftaten.[426] Der Katalog ist abschließend und erfasst unter anderem Straftaten des Friedensverrats, der Gefährdung des demokratischen Rechtsstaates, die Bildung einer terroristischen Vereinigung, Tötungsdelikte sowie sonst schwere Straftaten und daraus resultierende Großgefahren.[427] Die jeweils vom Katalog abgedeckten Delikte können zu einem überwiegenden Teil auf aktuelle Ereignisse und Bedrohungslagen zurückgeführt werden. Die Einfügung der Tötungsdelikte beruht beispielsweise auf dem Bombenattentat auf dem Münchner Oktoberfest im September 1980; die Übernahme der Brandschutzdelikte kann auf rechts- wie linksextremistisch motivierte Brandanschläge[428] zurückgeführt werden und die Einführung der §§ 239a, 239b, 315 III StGB und §§ 316b, 316c StGB wurde durch die Angst vor Geiselnahmen, Flugzeugentführungen und Übergriffe auf Castor-Transporte durch gewaltbereite linksextreme Gruppen begünstigt.[429]

Die parallele strafprozessuale Befugnis nach § 100a StPO ist auf ähnliche Anlasstaten begrenzt.[430] Allerdings muss die Anlasstat nach § 100a I Nr. 2 StPO im konkreten Einzelfall und nicht nur nach allgemeiner Erfahrung schwerwiegend und erheblich sein. Für die nachrichtendienstliche Überwachung genügt demgegenüber eine bloß abstrakt schwerwiegende Straftat, sofern diese einen ausdrücklichen Bezug zu den in § 1 I Nr. 1 G10 erwähnten Rechtsgütern aufweist.[431] Da es sich bei den Katalogtaten des G10 zumeist um Staatsschutzdelikte handelt, ist diese Bedingung regelmäßig erfüllt. Dem Vorliegen der Katalogtat kommt damit eine Indizwirkung zu, sofern nicht der Bagatellcharakter der Straftat dem entgegensteht.[432]

Die strategische Kontrolle richtet sich nach §§ 1, 5 G10. § 5 G10 erfordert in materieller Hinsicht eine bloße Eignungsprüfung. Danach müssen die für den Stichwortabgleich eingesetzten Suchbegriffe zur Aufklärung der enumerativ genannten Gefahrenbereiche „bestimmt und geeignet“ sein, ohne dass es in materieller Hin-

---

[426] Daneben kann die Überwachung auf dem Verdacht beruhen, dass der Betroffene Mitgliede einer Vereinigung ist, deren Zweck die Begehung von Straftaten gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes ist, § 3 I 2 G10.

[427] Vgl. BT-Drs. 17/4278, S. 4.

[428] So etwa die Brandanschläge in Hoyerswerda 1991 und Rostock-Lichtenhagen 1992; vgl. BT-Drs. 13/7164, S. 53ff; *T. Wollweber,* S. 195.

[429] Vgl. hierzu BT-Drs. 14/5655, S. 15. Daneben muss sich die Überwachung gegen eine der in § 3 II G10 genannten Personen richten. Dies sind insbesondere der Verdächtige selbst oder Personen, die mit dem Kommunikationsvorgang in Verbindung stehen. Letzteres kann aus der Entgegennahme oder Weitergabe der Mitteilungen sowie der Anschlussnutzung resultieren. Im Übrigen sind der Subsidiaritätsgedanke nach § 3 II 1 G10, der Kernbereichsschutz nach § 3a G10 sowie die formellen Anforderungen der §§ 9, 10, 15 VI G10 zu beachten.

[430] Die Subsidiaritätsklausel findet sich in § 100a I Nr. 3 StPO.

[431] Vgl. hierzu *Droste,* Handbuch, S. 336.

[432] Vgl. Borgs-Maciejewski/Ebert-*Borgs*, § 2 G10 Rn. 2.

sicht weiterer besonderer Voraussetzungen bedarf.[433] Die tauglichen Gefahrentatbestände werden in § 5 I 3 G10 abschließend genannt und erfordern eine erhebliche Bedeutung mit unmittelbarem Bezug zur Bundesrepublik Deutschland. Dazu gehört etwa die Gefahr eines bewaffneten Angriffs, der Begehung internationaler terroristischer Anschläge, der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen, der illegalen Einfuhr von Betäubungsmitteln in Fällen von erheblicher Bedeutung sowie der Beeinträchtigung der Geldwertstabilität. Sämtlichen dieser Gefahren muss nach § 1 I Nr. 2 G10 i.V.m. § 1 II BNDG außen- und sicherheitspolitische Bedeutung zukommen. Abgesehen von den restriktiven Gefahrtatbeständen unterliegt die automatisierte, anlassunabhängige Überwachung des Telekommunikationsverkehrs damit vergleichsweise geringen materiellen Anforderungen. Diese werden allerdings durch formale Anordnungs- und Kontrollmechanismen ergänzt, die bei der nachfolgenden Darstellung der verschiedenen Kontrollmechanismen eingehender untersucht werden sollen.

ee) Zwischenergebnis zu Erhebungsvoraussetzungen

Insgesamt sind die Anordnungsvoraussetzungen der Nachrichtendienste damit relativ vage gehalten. Während vergleichbare Maßnahmen nach der StPO an unterschiedliche Anlasstaten anknüpfen, wird im Nachrichtendienstrecht auf vergleichbar konkrete Straftatkataloge verzichtet.[434] Der Einsatz nachrichtendienstlicher Mittel wird vielmehr einheitlich in den §§ 8, 9 BVerfSchG geregelt. Eine Einschränkung wird lediglich über die Bindung an abstrakte Gefahrenlagen oder allgemeine Subsidiaritätserwägungen erzielt. Diese Vagheit und Abstraktheit trägt zu einer gewissen Übersichtlichkeit der geheimdienstlichen Vorschriften bei und führt zu einer Intransparenz bei der Wahrnehmung geheimdienstlicher Aufgaben.

f) Kontrollmechanismen und Verfahrensablauf

Das Vertrauen in Geheimdienstinformationen ist maßgeblich von der Existenz ausreichender Kontrollmechanismen abhängig. Dieses Vertrauen ist für eine rechtliche Nutzung der erlangten Beweise von erheblicher Bedeutung. Die nachfolgende Darstellung gibt einen Überblick über die wesentlichen Kontrollorgane und Kontrollmechanismen, die im Vorfeld beziehungsweise im Anschluss an eine nachrichtendienstliche Überwachung greifen können. Hierbei wird der Vergleich zum Strafverfolgungssektor gezogen.

---

[433] So § 5 II 1 G 10; vgl. hierzu *Grawe,* S. 125. Aus diesem Grund wird diese Methode u.a. als „elektronischer Staubsauger" bezeichnet, vgl. *Kühne,* Strafprozessrecht, Rn. 389.

[434] Zur Unübersichtlichkeit des Strafverfahrensrechts siehe *Zöller,* StraFo 2008, S. 19.

aa) Relevante Kontrollinstanzen

Die verschiedenen Kontrollorgane der Nachrichtendienste können jeweils einer der drei Staatsgewalten zugeordnet werden.[435] In Bezug auf die Exekutivkontrolle ist zwischen internen und externen Kontrollmechanismen zu unterscheiden.[436] Intern unterliegen die deutschen Nachrichtendienste der Dienst- und Fachaufsicht der jeweiligen Ministerien. Diese Aufgabe wird für das BfV durch das BMI, für den MAD durch das BMVg und für den BND durch das Bundeskanzleramt wahrgenommen. Im Kanzleramt ist zudem der Beauftragte für die Nachrichtendienste angesiedelt, dem unter anderem die Koordination der verschiedenen Dienste obliegt.[437] Im Bereich der externen Kontrolle stellt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Einhaltung datenschutzrechtlicher Vorgaben durch die Nachrichtendienste sicher. Die Budgetkontrolle wird durch das sogenannte Dreier-Kollegium des Bundesrechnungshofs übergenommen.[438] Die daneben bestehende Rechtskontrolle erfolgt unter anderem durch die verwaltungsgerichtliche Nachprüfung nachrichtendienstlicher Einzelmaßnahmen sowie die gerichtliche Durchsetzung möglicher Auskunftsansprüche nach 15 BVerfSchG.[439] Je nach Klagebegehren kann zudem der Rechtsweg zu den Zivilgerichten offenstehen. Die klassische parlamentarische Kontrolle erfasst schließlich Institute wie die Anfrage, die aktuelle Stunde, Petitionen und Untersuchungsausschüsse.[440] Für Eingriffe in die Unverletzlichkeit der Wohnung kann nach Art. 13 VI 2 GG zusätzlich ein parlamentarisches Kontrollorgan errichtet werden, das die sonstigen parlamentarischen Kontrollinstanzen ergänzt.[441] Diese Kontrollmechanismen finden üblicherweise in der Öffentlichkeit statt.[442] Die hiermit verbundene Transparenz widerspricht jedoch in den meisten Fällen den im Geheimdienstsektor bestehenden Geheimhaltungsinteressen. Selbst die geheim tagenden Abteilungen des Innen-

---

[435] Daneben erfolgt durch individuelle Auskunftsansprüche, Medien, Verfassungsschutzberichte und Öffentlichkeitsarbeit ergänzend eine öffentliche Kontrolle. Diese ist aufgrund der besonderen Geheimhaltungserfordernisse im Geheimdienstsektor sehr selektiv und keinesfalls umfassend. Sie betrifft zumeist öffentlich bekannt gewordene Misserfolge, vgl. *Baier,* S. 88.

[436] Vergleiche hierzu jeweils *Droste,* Handbuch, S. 611ff, 616ff.

[437] Vgl. *Droste,* Handbuch, S. 612f; *Rose-Stahl,* S. 164.

[438] Vgl. *Rose-Stahl,* S. 164.

[439] Vertiefend *Droste,* Handbuch, S. 602; *Gusy,* Grundrechte, S. 85ff.

[440] Vertiefend zur parlamentarischen Kontrolle der Nachrichtendienste vgl. *Bull,* DöV 2008, S. 751ff; *Gusy,* ZRP 2008, S. 36ff; *Gusy,* Grundrechte, S. 121ff.

[441] Vgl. BT-Drs. 13/8650, S. 5. Vertiefend *Hörauf,* S. 162f, 351; Maunz/Dürig-*Papier,* Art. 13 Rn. 117f. Die strategische Kontrolle ist mit einer nur geringen Rechtsschutzfunktion verbunden. Aufgrund der Inlandsbezogenheit ist sie weitgehend auf den MAD und das BfV begrenzt. Insgesamt kommt dem Gremium eine nur geringe praktische Relevanz zu, sodass es nachfolgend weitgehend außer Betracht bleibt; vgl. *Brissa,* DöV 2011, S. 392; BT-Drs. 16/6363, 16/10300, 16/14116, 17/3038.

[442] Zur Öffentlichkeit vgl. Art. 42 I 1 GG.

ausschusses bieten aufgrund der großen Anzahl der Beteiligten keinen ausreichenden Geheimnisschutz. Aus diesem Grund wurden für den Nachrichtendienstsektor mit dem Parlamentarischen Kontrollgremium (PKGr)[443] und der G10-Kommission spezielle Kontrollorgane geschaffen, welche die Schwächen der klassischen Kontrollmechanismen überwinden sollen.[444]

Das PKGr kontrolliert die Bundesregierung hinsichtlich der Tätigkeit ihrer Nachrichtendienste.[445] Es tritt ergänzend neben die klassischen parlamentarischen Kontrollinstanzen und stützt sich auf die Ermächtigungen im Kontrollgremiumsgesetz (PKGrG), dem BVerfSchG und dem G10.[446] Die Mitglieder des Gremiums werden durch den Bundestag zu Beginn jeder Wahlperiode aus der Mitte des Bundestags gewählt, § 2 I PKGrG. Um den Geheimhaltungsbedürfnissen des Nachrichtendienstwesens Rechnung zu tragen, sind die Beratungen des Gremiums geheim. Die Kompetenz und Vertrauenswürdigkeit der involvierten Personen wird durch ein besonderes Auswahlverfahren sichergestellt.[447] Die Mitglieder sind auch nach ihrem Ausscheiden aus dem Gremium zur Geheimhaltung verpflichtet, § 10I PKGrG.

Die G10-Kommission agiert in einem Überschneidungsbereich parlamentarischer, exekutiver und gerichtlicher Kontrolle, ohne dass sie einer der drei Gewalten zugeordnet werden kann.[448] Sie verfügt als „Kontrollorgan eigener Art" über eigenständige Kontroll- und Mitentscheidungsaufgaben.[449] Sie setzt sich aus einem Vorsitzenden mit der Befähigung zum Richteramt sowie drei Beisitzern und vier stellvertretenden Mitgliedern zusammen. Die Kommissionsmitglieder werden vom PKGr nach Anhörung der Bundesregierung bestellt. Sie selbst müssen dem Bundestag nicht angehören.[450] Inhaltlich ist die G10-Kommission für die Überwachung der Recht- und Zweckmäßigkeit von Maßnahmen nach dem G10 zuständig.[451] Die Kommissionsmitglieder treffen ihre Entscheidungen weisungsunabhängig und in geheimer Sitzung.[452]

---

[443] Die ursprüngliche Bezeichnung als „Parlamentarische Kontrollkommission" (PKK) wurde 1999 durch die heutige Bezeichnung ersetzt; vgl. *Droste,* Handbuch, S. 624.

[444] Vertiefend *Baier,* S. 72, 91.

[445] Vgl. *Baier,* S. 82; *Droste,* Handbuch, S. 627. Vertiefend *Roggan,* G10 Rn. 1ff.

[446] So § 1 II PKGrG sowie *Baier,* S. 82f. Die grundgesetzlich verbürgten Rechte des Bundestages können nicht durch einfaches Bundesrecht ausgehebelt werden.

[447] Vgl. *Baier,* S. 87.

[448] So bereit BVerfG NJW 1971, S. 275; vgl. zudem *Gusy,* Grundrechte, S. 17, 19. Insgesamt vertiefend bei *Roggan*, G10 § 15 Rn. 1ff.

[449] Vgl. BVerfG NJW 1971, S. 275, Leitsatz h). Ebenso *Baier,* S. 91; *Gusy,* Grundrechte, S. 17; *Huber,* NJW 2007, S. 882.

[450] Vgl. BVerfG NJW 1971, S. 275, 278.

[451] Vgl. hierzu § 15 V G10 sowie *Droste,* Handbuch, S. 641; *Rehbein,* S. 111. Vertiefend *Gusy,* Grundrechte, S. 15ff, 59ff.

[452] § 15 I 1, 3, 4, II G10.

Die vergleichsweise zu betrachtenden Strafverfolgungsbehörden sind ebenfalls in klassische Dienst- und Rechtskontrollen eingebunden. In diesem Sinne unterliegen die Staatsanwaltschaften nach den §§ 146, 147 GVG etwa den Weisungen und der Dienstaufsicht der ihr vorgesetzten Stellen. Durch sogenannte Dienstaufsichtsbeschwerden können Maßnahmen der Staatsanwaltschaften überprüft werden.[453] Dem PKGr oder der G10-Kommission vergleichbare spezielle Kontrollgremien sind nicht vorhanden.

bb) Präventiv- beziehungsweise Vorabkontrolle

Vor der Durchführung einer nachrichtendienstlichen Informationserhebung können in Abhängigkeit von der Erhebungsbefugnis unterschiedliche Kontrollmechanismen greifen. Denkbar sind die Begrenzung der Antrags- und Anordnungskompetenzen sowie eine Bindung an gerichtliche Zustimmungserfordernisse. Derartige Vorabkontrollen bilden im deutschen Rechtssystem die Ausnahme vom Grundsatz des nachträglichen Rechtsschutzes und bedürfen daher regelmäßig einer ausdrücklichen Anordnung.[454] Derartige Ausnahmen können sich direkt aus dem Grundgesetz oder aus allgemeinen rechtlichen Erwägungen ergeben. Das Grundgesetz geht etwa bei Eingriffen in die Unverletzlichkeit der Wohnung und die persönliche Freiheit von der Notwendigkeit einer vorherigen Einzelfallkontrolle aus.[455] Im Übrigen kann eine vorherige richterliche Rechtmäßigkeitskontrolle bei besonderer Eingriffsintensität aus Gründen der Verhältnismäßigkeit geboten sein.[456] Daneben können Aspekte der Fairness und Chancengleichheit vor allem bei heimlichen Ermittlungsmaßnahmen für eine Präventivkontrolle sprechen. In der letzteren Konstellation soll der Richter als neutrale Instanz das tatsächliche Vorliegen der Anordnungsvoraussetzungen im Zeitpunkt der Anordnung und die Rechtmäßigkeit des damit verbundenen Informationsvorsprungs sicherstellen.[457]

Diese präventiven Kontrollmechanismen sind im Geheimdienstsektor unterschiedlich stark ausgeprägt. Im Einzelnen muss zwischen der Vorabkontrolle im Anwendungsbereich der Nachrichtendienstgesetze einerseits und dem G10 andererseits unterschieden werden.

---

[453] Vgl. KK-*Schmid/Schoreit,* § 147 GVG Rn. 5.

[454] In diesem Sinne geht auch die Vorschrift des Art. 19 IV GG im Grundsatz von der Garantie eines *nachträglichen* Rechtsschutzes aus, vgl. *Gusy,* JZ 1998, S. 167.

[455] Vgl. Art. 13 II, III, IV, 104 II 1 GG.

[456] Vgl. vertiefend zum vorbeugenden Rechtsschutz *Gusy,* JZ 1998, S. 168f.

[457] Vgl. *Meier,* ZRP 2010, S. 225. Zu Sinn und Zweck des Richtervorbehalts vgl. *Brüning,* HRRS 2007, S. 252f.

(1) Einsatz Verdeckter Ermittler

Der Einsatz heimlicher Ermittlungsmethoden durch die Nachrichtendienste nach §§ 8 II, 9 I BVerfSchG sieht keine besonderen formellen Antrags- oder Anordnungsvoraussetzungen vor. Maßnahmen wie beispielsweise der Einsatz eines UCAs bedürfen lediglich einer vorherigen behördeninternen Zustimmung.[458]

Im Vergleich dazu erfordert der Einsatz eines VE nach der Strafprozessordnung neben der Zustimmung des polizeilichen Dienstvorgesetzten zusätzlich die Zustimmung der Staatsanwaltschaft.[459] Einsätze gegen einen bestimmten Beschuldigten oder das Betreten der Wohnung stehen sogar unter Richtervorbehalt.[460] Ähnliche Vorgaben enthalten sämtliche Vorschriften der Strafprozessordnung zu eingriffsintensiven, heimlichen Ermittlungsmaßnahmen,[461] während der Einsatz nachrichtendienstlicher Mittel keinen vergleichbaren Vorabkontrollen unterworfen ist. Zwar sollte der strafprozessuale Richtervorbehalt in seiner Effektivität ebenfalls nicht überschätzt werden, dennoch sind bei einer vergleichenden Betrachtung die präventiven Kontrollmechanismen für heimliche Ermittlungsmethoden im Nachrichtendienstbereich deutlich schwächer ausgebildet.[462]

Die unterschiedliche Ausgestaltung präventiver Kontrollmechanismen wird auch in der Literatur kritisch diskutiert.[463] Nach Ansicht vereinzelter Kritiker müsse bereits aufgrund der im Nachrichtendienstsektor abgeschwächten präventiven Kontrollmechanismen eine beweisrechtliche Nutzung ausscheiden. Die Nutzung von Geheimdienstinformationen durch die Strafverfolgungsbehörden könnte den im Strafverfahrensrecht angelegten Schutz der richterlichen Vorabkontrolle umgehen. Die vorgebrachten Bedenken verlieren jedoch an Schlagkraft, sobald man die tatsächliche Effektivität des strafprozessualen Richtervorbehalts in die Beurteilung mit einbezieht.[464] Die Schutzwirkung des Richtervorbehalts wird durch die unzureichende Wahrnehmung der Kontroll-, Begründungs- und Dokumentationspflichten erheblich geschwächt. Etwaige Defizite äußern sich beispielsweise in Begrün-

---

458 Vgl. *Droste,* Handbuch, S. 278.

459 Vgl. § 110b I 1 StPO.

460 Vgl. § 110b II 1 StPO sowie *Roggan,* in: Roggan/Kutscha, S. 191.

461 Beispiele hierfür sind die §§ 98b, 110b I, II, 163d II StPO. Davon abgesehen existieren nur wenige formfreie Anordnungen, wie z.B. der Datenabgleich nach § 98c StPO.

462 Vgl. zu den Schwächen des strafprozessualen Richtervorbehalts *Asbrock,* KritV 1997, S. 255ff; *Roggan,* in: Roggan/Kutscha, S. 191f.

463 Vgl. *Hefendehl,* GA 2011, S. 229. Zur Bedeutung des Richtervorbehalts als neutrale Kontrolle zum Schutz vor unverhältnismäßigen Grundrechtseingriffen, vgl. *Schnarr,* NStZ 1991, S. 210.

464 Zu den Zweifeln vgl. *Asbrock,* KritV 1997, S. 255ff*; Gusy,* JZ 1998, S. 168. Nach *Backes/Gusy,* S. 45, genügen nur 75 % der Richterbeschlüsse den gesetzlichen Ansprüchen.

dungsmängeln[465] oder der fehlenden Korrektur mangelhafter Antragsformulare.[466] Diese Mängel resultieren neben Personal- und Zeitmangel aus einer unzureichenden Kenntnis des tatsächlichen Sachverhalts.[467] In der Folge werden die beantragten Maßnahmen nur auf ihre Schlüssigkeit hin geprüft, sodass Ermittlungsmaßnahmen nur selten abgelehnt werden.[468] Darüber hinaus wird der Richtervorbehalt durch die überproportionale Heranziehung von Eilkompetenzen der Staatsanwaltschaft entwertet.[469]

(2) Wohnraumüberwachung

Erhöhte Anforderungen gelten im Nachrichtendienstrecht allerdings bei Eingriffen in Art. 13 GG. Bei einer akustischen Wohnraumüberwachung nach §§ 8 II, 9 II BVerfSchG ist beispielsweise die Anordnungsbefugnis dem Gericht beziehungsweise in Eilfällen dem Präsidenten des BfV oder seinen Stellvertreter vorbehalten.[470] Bei Wahrnehmung der Eilkompetenz ist die richterliche Entscheidung unverzüglich nachzuholen.[471] Weiterhin unbeschränkt ist die Antragsbefugnis.

Die Parallelnorm des § 100d I 1 StPO im Strafverfahrensrecht weist die Anordnungskompetenz demgegenüber einer besonderen Strafkammer des Landgerichts zu. Selbst in Eilfällen muss dort die Anordnung durch den Vorsitzenden der Strafkammer erfolgen und ist innerhalb von drei Werktagen durch die Strafkammer zu bestätigen.[472] Die formalen Anforderungen sind damit im Nachrichtendienstrecht weiterhin etwas niedriger angesetzt als im Strafverfahrensrecht. Dieser bei der nachrichtendienstlichen Wohnraumüberwachung schwächere Richtervorbehalt wird bereits durch die innere Systematik des § 9 II BVerfSchG angedeutet, die zunächst die Eil- und erst danach die Regelkompetenz benennt. Diese Reihenfolge

---

[465] Praktisch äußern sich etwaige Begründungsmängel beispielsweise durch eine wörtliche Übernahme staatsanwaltschaftlicher Beschlussentwürfe. Diese erfolgt in über 90 % der beantragten Telefonüberwachungsmaßnahmen, vgl. *Backes/Gusy,* S. 47.

[466] Vgl. dazu *Roggan,* in: Roggan/Kutscha, S. 193, der auf den Fall vor dem BGH, NStZ 1997, S. 249f, verweist, in dem ein dem Richter vorgelegtes Formular an der falschen Stelle angekreuzt war und der Richter diesen Fehler nicht korrigierte.

[467] Vgl. *Zöller,* StraFo 2008, S. 21. Die Defizite resultieren u.a. aus der einseitigen bzw. gefilterten Sachverhaltsdarstellung der beantragenden Behörde sowie dem Fehlen eigenständiger Aufklärungsmöglichkeiten des Gerichts, vgl. *Gusy,* JZ 1998, S. 173.

[468] So *Gusy,* JZ 1998, S. 171. In der Studie von *Backes/Gusy* erfolgte eine Ablehnung sogar nur in 0,3 % der Fälle, vgl. *Backes/Gusy,* S. 44.

[469] Vgl. *Asbrock,* KritV 1997, S. 258; *Zöller,* StraFo 2008, S. 20.

[470] Vgl. § 8 II 2, 3 BVerfSchG. Der dort genannte Richtervorbehalt geht auf die Änderungen des Art. 13 IV GG durch das Gesetz vom 26.3.1998 zurück, BGBl. I, 1998, S. 610. Dieser knüpft die technische Wohnraumüberwachung generell an das Vorliegen einer richterlichen Anordnung, vgl. hierzu *Droste,* Handbuch, S. 317.

[471] Vgl. § 8 II 4 BVerfSchG.

[472] Vgl. § 100d I 2, 3 StPO.

legt nahe, dass das Gesetz die Eilkompetenz als Regelfall und den Richtervorbehalt als Ausnahmefall einstuft.

(3) Auskunftsersuchen

Weitere Besonderheiten ergeben sich in Bezug auf ein Auskunftsersuchen nach § 8a BVerfSchG. In § 8a BVerfSchG sieht die Vorabkontrolle sowohl eine eingeschränkte Antrags-, als auch Anordnungsbefugnis vor. Nach § 8b I BVerfSchG darf lediglich der Behördenleiter oder sein Stellvertreter eine Auskunft nach § 8a BVerfSchG beantragen. Die Anordnungskompetenz liegt wiederum allein beim BMI, dem insofern eine Aufsichtsfunktion zukommt.[473] Darüber hinaus ist zum Teil sogar eine Unterrichtung der G10-Kommission erforderlich, damit diese vor Vollzug der Maßnahme die Zulässigkeit und Notwendigkeit der Auskunft überprüfen kann.[474] Die im Vergleich zu sonstigen nachrichtendienstlichen Maßnahmen verschärfte Vorabkontrolle ist der besonderen Eingriffsintensität der Maßnahmen geschuldet.

Diese Kontrollintensität deckt sich mit den Wertungen im Strafverfahrens- und Polizeirecht.[475] Diese sehen bei vergleichbar intensiven Eingriffen einen Richtervorbehalt vor.

(4) Telekommunikationsüberwachung

Die striktesten Vorabkontrollen gelten für Überwachungsmaßnahmen nach dem G10. Diese sind in einen komplexen Kontrollprozess aus verschiedenen internen Kontrollvorgängen, Antrags-, Anordnungs- und Zustimmungserfordernissen sowie begleitenden Aufsichtsmaßnahmen eingebunden.[476] Die interne Kontrolle wird beispielsweise durch sogenannte „G10-Stellen“ wahrgenommen, welche Post- und Telekommunikationsdaten einer Vorprüfung unterziehen. Diese innerhalb des Verfassungsschutzes angesiedelten Abteilungen überprüfen die Daten auf ihre nachrichtendienstliche Relevanz.[477] Die Freigabe an die Fachabteilungen erfolgt erst, wenn zusätzlich ein Angestellter des Dienstes mit der Befähigung zum Richteramt die Verwertbarkeit der Daten überprüft hat.[478] Diese internen Kontrollvorgänge werden durch zahlreiche externe Kontrollmechanismen ergänzt. In diesem Zusammenhang spielt die sogenannte G10-Kommission eine zentrale Rolle. Der Vollzug

---

473 BT-Drs. 17/6925, S. 14f.

474 § 8b II BVerfSchG.

475 Vgl. sinngemäß BT-Drs. 17/6925, S. 15.

476 Vgl. hierzu die §§ 1 II, 9, 10 G10 sowie insgesamt *Baier,* S. 90ff.

477 Vgl. *Albert,* in: Korte/Zoller, S. 99f.

478 Vgl. *Albert,* in: Korte/Zoller, S. 99f; *Droste,* Handbuch, S. 347f.

einer G10-Maßnahme erfordert grundsätzlich die vorherige Zustimmung der Kommission, welche die Beschränkungsmaßnahme zu diesem Zweck einer Einzelfallkontrolle unterzieht.[479] Ausnahmen werden nur bei Gefahr im Verzug gestattet, wobei die Bestätigung der Kommission unverzüglich nachzubeantragen ist.[480] Der G10-Kommission stehen zur Wahrnehmung ihrer Kontrollfunktion die in § 15 V 3 G10 genannten Auskunfts-, Einsichts- und Zutrittsrechte zur Verfügung.

Im Einzelnen muss eine G10-Überwachung vor ihrer Durchführung die nachfolgend aufgeführten Kontrollinstanzen durchlaufen. In einem ersten Schritt muss der Behördenleiter beziehungsweise sein Stellvertreter nach § 9 G10 beim zuständigen Bundesministerium einen schriftlich begründeten Antrag auf Anordnung der Maßnahme stellen.[481] Dieser Antrag wird in einem zweiten Schritt vom Ministerium überprüft und bei einer positiven Entscheidung dem Antrag entsprechend angeordnet.[482] Diese Entscheidung teilt das Ministerium vor Vollzug der Maßnahme der G10-Kommission mit, welche die Anordnungsentscheidung in einem dritten Schritt einer Einzelfallkontrolle unterzieht.[483] Dogmatisch handelt es sich bei der zu überprüfenden Anordnung des Ministeriums um einen mehrstufigen Verwaltungsakt, für dessen Wirksamkeit grundsätzlich die Mitwirkung der G10-Kommission in Form der Zustimmung erforderlich ist. Die Durchführung der angeordneten Beschränkungsmaßnahme ist damit von der Zustimmung der G10-Kommission abhängig. Wird die Zustimmung vor Vollziehung verweigert, führt dies zur Erledigung des Verwaltungsaktes.[484] Wird die Zustimmung erteilt, kann die Überwachung durchgeführt werden. Diese erfolgt in einem vierten Schritt unter der begleitenden Aufsicht eines Bediensteten mit der Befähigung zum Richteramt.[485] Im Übrigen ist der Rechtsweg gegen die Anordnung vor einer Mitteilung an den Betroffenen nach § 13 G10 ausdrücklich ausgeschlossen.[486] Da der Betroffene aufgrund der weitgehenden Geheimhaltung von der Maßnahme – wenn überhaupt – erst im Nachhinein Kenntnis erhält, führt diese Vorschrift faktisch zu einem Ausschluss der richterlichen Vorabkontrolle.[487]

Das beschriebene Kontrollverfahren ist letztlich nicht als Rechtsweg i.S.d. Art. 19 IV 1 GG konzipiert. Diese Abweichung vom Richtervorbehalt wird in

---

[479] Vgl. hierzu *Baier,* S. 93.

[480] Vgl. § 15 VI 1, 2 G10.

[481] Bei Anträgen der Landesverfassungsschutzbehörden ist für die Überprüfung und Anordnung die zuständige oberste Landesbehörde berufen, § 10 I G10.

[482] Vgl. § 10 I G10.

[483] Vgl. § 15 VI 1 G10 sowie *Droste,* Handbuch, S. 346.

[484] Vgl. *Droste,* Handbuch, S. 346 und S. 641 Fn. 118.

[485] Vgl. § 11 I G10.

[486] Vertiefend *Roggan*, G10, § 13 Rn. 1ff.

[487] *Roggan,* G10 § 12 Rn. 6 verweist auf das quantitative Überwiegen der Ausnahmen von der Mitteilungspflicht.

Art. 10 II 2, 19 IV 3 GG als zulässig anerkannt. Danach erfordert die Kontrolle durch eine unabhängige Instanz nicht zwingend die Einschaltung eines Richters, vielmehr kann er durch bestimmte andere Organe beziehungsweise Hilfsorgane ersetzt werden.[488] Die G10-Kommission wurde vom Bundesverfassungsgericht aufgrund ihrer Unabhängigkeit sowie Sach- und Rechtskunde als ein derartiges Organ und ihre Tätigkeit damit als gleichwertiger Ersatz für eine gerichtliche Kontrolle anerkannt.[489] Begründet wird diese Sonderbehandlung mit dem Erhalt eines funktionsfähigen Verfassungsschutzes, der bei seiner Arbeit grundsätzlich auf einen ausreichenden Geheimnisschutz angewiesen sei.[490] Der vorgenannte Ausschluss der richterlichen Vorabkontrolle werde durch die ausgedehnte Vorabkontrolle der G10-Kommission kompensiert. Die G10-Kommission nimmt in diesem Zusammenhang gerichtsähnliche Aufgaben wahr.[491] Diese Vorabkontrolle nach dem G10 ist insgesamt weitaus komplexer als der im Strafprozessrecht für vergleichbare Maßnahmen geltende Richtervorbehalt.[492]

Eine präventive Kontrolle durch das PKGr scheidet demgegenüber aus. Der Grundsatz der Gewaltenteilung verlangt die funktionale Unabhängigkeit und eigenverantwortliche Aufgabenwahrnehmung durch die verschiedenen Staatsgewalten. Die nachrichtendienstliche Tätigkeit unterliegt als exekutives Handeln allein der Fachaufsicht der Regierung.[493] Im Vorfeld einer Maßnahme kann das PKGr als Teil der Legislative lediglich durch die Aufstellung allgemeiner Leitlinien auf die Arbeit der Dienste Einfluss nehmen. Dies ist etwa durch den Erlass der Dienstvorschrift i.S.d. § 8 II 2, 3 BVerfSchG möglich.[494] Diese Dienstvorschrift unterliegt allerdings der Geheimhaltung, sodass die Legitimationskette nicht offengelegt wird. Daneben kann das PKGr mittelbar auf die Reichweite der strategischen Überwachung Einfluss nehmen. Nach §§ 5 I 2, 8 II 1 G10 bedarf die Bestimmung der überwachbaren Telekommunikationsbeziehungen der Zustimmung des PKGr.[495] Eine darüber hinausgehende Einwirkung im Vorfeld einer Maßnahme ist dem PKGr dagegen nicht gestattet. Die Befugnisse des PKGr beziehen sich vorwiegend auf abgeschlossene Vorgänge und sind damit auf eine nachträgliche

---

488 So *Droste,* Handbuch, S. 643.

489 Vgl. BVerfG NVwZ 1994, S. 367; *Droste,* Handbuch, S. 643f. Diese Lösung steht zudem mit Art. 8 II EMRK im Einklang, so *Schäfer,* S. 142.

490 Vgl. BVerfGE 30, 1, 18f.

491 Vgl. *Bull,* Datenschutz, S. 83 Fn. 194.

492 Vgl. etwa die §§ 100a, 100b StPO.

493 Vgl. *Peitsch/Polzin,* NVwZ 2000, S. 388.

494 Diese Dienstvorschrift bedarf der Zustimmung des BMI, der das PKGr unterrichtet; vgl. *Droste,* Handbuch, S. 627.

495 Vgl. *Baier,* S. 96.

Kontrolle angelegt.[496] Dieses soll primär die Rechtmäßigkeit staatlichen Handelns und nicht individuellen Rechtsschutz gewährleisten.[497]

Ein Vergleich zu Überwachungsmaßnahmen der Strafverfolgungsbehörden ist nur bedingt möglich, da diesen nur im Einzelfall der Zugriff auf Inhaltsdaten von Telekommunikationsvorgängen gestattet ist. Für diesen eng umrissenen Bereich ist nach den §§ 100a, 100b StPO eine richterliche Anordnung erforderlich und ausreichend. Die Vorabkontrolle der Telekommunikationsüberwachung durch die Nachrichtendienste ist im Vergleich damit deutlich intensiver als für die Telekommunikationsüberwachung der Strafverfolgungsbehörden. Die in materieller Hinsicht geringeren Anforderungen werden dementsprechend durch einen komplexeren und strikteren Genehmigungsprozess kompensiert.[498] Dies führt dazu, dass die Individualüberwachung nach § 3 G10 weitaus seltener erfolgt als eine strafprozessuale Telekommunikationsüberwachung nach den §§ 100a, 100b StPO. Zum Teil ist von einem Verhältnis von 1:100 die Rede.[499]

(5) Zwischenergebnis

Die im Nachrichtendienstrecht bestehenden Kontrollmöglichkeiten sind je nach Art der Erhebungsmethode unterschiedlich stark ausgeprägt. Für die Informationserhebung nach den Nachrichtendienstgesetzen sind die gesetzlich vorgesehenen präventiven Kontrollmechanismen deutlich schwächer ausgebildet als für vergleichbare Maßnahmen nach der Strafprozessordnung. Während das Strafverfahrensrecht beispielsweise bei besonders eingriffsintensiven Erhebungsmaßnahmen in der Regel einen Richtervorbehalt vorsieht, ist die Anordnungskompetenz im Geheimdienstsektor oftmals der Behördenleitung übertragen. Allerdings fallen die in den Nachrichtendienstgesetzen zum Teil geringeren Vorabkontrollen aufgrund der erheblichen Schwächen des strafprozessualen Richtervorbehalts praktisch nicht so sehr ins Gewicht. Selbst im Einzelfall fehlende Vorabkontrollen sind nicht von vorneherein bedenklich. Die verfassungsrechtliche Garantie eines effektiven Rechtsschutzes stützt sich grundsätzlich auf das Vorhandensein nachträglicher Rechtsschutzmöglichkeiten.[500] Dem Gesetzgeber ist bei der konkreten Ausgestaltung dieses Rechtsschutzes daher eine gewisse Einschätzungsprärogative zuzugestehen. Für Überwachungsmaßnahmen nach dem G10 ist die Kontrolldichte dem-

---

496 Vgl. BVerfG NJW 1984, S. 2271, 2275, sowie *Peitsch/Polzin,* NVwZ 2000, S. 389.

497 Vgl. BVerfG NJW 1984, S. 2271, 2275, mit dem Verweis, dass es sich um eine politische und keine „administrative Überkontrolle" handelt.

498 Vgl. *Droste,* Handbuch, S. 300.

499 Vgl. *Albert,* in: Korte/Zoller, S. 101; *Droste,* Handbuch, S. 344; BT-Drs. 17/4278, S. 5, sowie die Statistik des Bundesamtes für Justiz für das Berichtsjahr 2009 unter http://www.bundesjustizamt.de.

500 Vgl. *Rehbein,* S. 277. Sinngemäß *Weßlau,* S. 206, allerdings mit Bedenken.

gegenüber erhöht. Dort wird die richterliche Kontrolle durch eine vorgeschaltete Zustimmung der G10-Kommission ersetzt, die als unabhängiges, gerichtsähnliches Gremium agiert.[501]

cc) Nachträgliche Kontrolle

Die nachträgliche Kontrolle im Geheimdienstsektor wird primär durch das PKGr, die G10-Kommission und die Gerichte wahrgenommen. Im Strafverfolgungssektor bestehen demgegenüber keine dem PKGr oder der G10-Kommission vergleichbaren Kontrollinstanzen.[502]

(1) Parlamentarisches Kontrollgremium

Das PKGr ist seinen Wesen nach ein parlamentarisches Kontrollinstrument. Die Kontrolle wird durch eine umfassende Unterrichtungspflicht der Bundesregierung sowie Einsichts-, Besuchs- und Anhörungsrechte des PKGr ermöglicht.[503]

Gegenstand der Kontrolle ist die Arbeit der Regierung hinsichtlich der Tätigkeit ihrer Dienste; nicht das Agieren der Dienste selbst. Kontrolliert werden „allgemeine Tätigkeiten" sowie „sonstige Vorgänge von besonderer Bedeutung". Das erste Merkmal erfasst typische Arbeitsabläufe und Ergebnisse, das zweite Merkmal betrifft Geschehnisse, die vom typischen Arbeitsablauf abweichen sowie aktuelle Vorgänge und Gefahrenlagen von besonderer Relevanz.[504] Um etwaige Kontrolllücken zu vermeiden, muss die Bundesregierung ergänzend über „sonstige Vorgänge" berichten.[505] Die Kontrolle durch das PKGr beschränkt sich damit insgesamt auf eine eher allgemeine politische Kontrolle und Angelegenheiten von genereller Bedeutung.[506] Der Berichtspflicht unterliegen zudem nur solche Informationen, über welche die Dienste selbst verfügungsbefugt sind. Eine derartige Berechtigung fehlt etwa bei Informationen, die von den Landesverfassungsschutzbehörden oder ausländischen Partnerdiensten stammen.[507] Ebenfalls ausgenommen sind Informa-

---

501 Vgl. *Bull,* Datenschutz, S. 83; *Huber,* NVwZ 2011, S. 411.

502 Neben der klassischen Dienstaufsicht und der Kontrolle im Rechtsmittelverfahren kommt eine nachträgliche Kontrolle von Strafverfolgungsmaßnahmen in der Regel nur auf Initiative von außen zustande. In diesem Sinne sind etwa Rügen der Verteidigung, die Beschwerde nach § 172 I StPO oder der Vorwurf der Rechtsbeugung nach § 339 StGB denkbar.

503 Siehe § 4 PKGrG. Das PKGr unterrichtet seinerseits halbjährlich den Bundestag über seine bisherige Kontrolltätigkeit, § 13 PKGrG.

504 Vgl. *Droste,* Handbuch, S. 628; *Peitsch/Polzin,* NVwZ 2000, S. 390.

505 Vgl. *Droste,* Handbuch, S. 628.

506 Vgl. *Peitsch/Polzin,* NVwZ 2000, S. 389f.

507 Vgl. § 6 I PKGrG. Diese Vorgabe ist dem Föderalismusprinzip geschuldet, vgl. *Peitsch/Polzin,* NVwZ 2000, S. 391.

tionen, die den Quellenschutz, Persönlichkeitsrechte Dritter oder den Kernbereich der exekutiven Eigenverantwortung betreffen.[508]

Die einzelnen Kontrollbefugnisse des Gremiums ergeben sich aus § 5 PKGrG. Danach können unter anderem die Herausgabe von Akten und Schriftstücken, die Übermittlung von Daten und der Zutritt zu sämtlichen Dienststellen verlangt werden. Zudem ist das PKGr befugt, von bestimmten Personen, wie Angehörigen der Nachrichtendienste, Mitarbeitern und Mitgliedern der Bundesregierung, nach Unterrichtung der Bundesregierung Auskünfte einzuholen. Diese Personen müssen vollständige und wahrheitsgemäße Angaben machen.[509] Darüber hinaus sind Gerichte und Behörden zur Rechts- und Amtshilfe verpflichtet.[510] Diese Befugnisse werden durch weitere Berichtspflichten der Nachrichtendienstgesetze und dem G10 ergänzt. Nach § 8b III BVerfSchG muss das BMI dem PKGrG halbjährlich über Anlass, Umfang, Dauer, Ergebnis und Kosten von Anordnungen nach § 8a BVerfSchG berichten. Gleiches gilt nach § 9 III Nr. 2 BVerfSchG für die Wohnraumüberwachung nach § 9 II BVerfSchG. Im Anwendungsbereich des G10 ist das PKGr zudem im Abstand von höchstens sechs Monaten über die Durchführung des G10-Gesetzes sowie über etwaige Übermittlungen an ausländische Stellen in Kenntnis zu setzen.[511] Dementsprechend handelt es sich bei Kontrolle durch das PKGr weniger um eine nachträgliche als vielmehr um eine begleitende und damit aufsichtsähnliche Kontrolle.[512]

Die Effektivität dieser Kontrollinstanz wird vereinzelt kritisch gesehen. Bedenken werden unter anderem mit Blick auf die Informationsabhängigkeit derartiger Kontrollinstanzen geäußert.[513] Aufgrund der Geheimhaltungsbedürftigkeit des Nachrichtendienstwesens seien die einzelnen Gremien und Regierungseinheiten auf Informationen von den Behörden angewiesen, die sie kontrollieren sollen.[514] Trotz des Vertrauens in die Rechtmäßigkeit staatlichen Handelns sei dieses Informationsmonopol aufseiten der Dienste beziehungsweise das Informationsgefälle im

---

508 Vgl. § 6 II PKGrG. Dies betrifft u.a. personenbezogene Daten aus einer Sicherheitsüberprüfung; vgl. insgesamt *Droste,* Handbuch, S. 630f; *Huber,* NVwZ 2009, S. 1322.

509 Vgl. § 5 II PKGrG.

510 Vgl. § 5 IV 1 PKGrG.

511 Vgl. § 14 I G10 und § 7a VI G10.

512 Vgl. *Baier,* S. 88; *Peitsch/Polzin,* NVwZ 2000, S. 389, dort unter dem Stichwort „mitlaufende Kontrolle". Diese aufsichtsähnliche Funktion wird zum Teil aufgrund des Gewaltenteilungsgrundsatzes kritisch gesehen, vgl. *Droste,* Handbuch, S. 627, 629.

513 Kritisch zur Definitionsmacht der Dienste *Droste,* Handbuch, S. 639.

514 Vgl. *Gusy,* ZRP 2008, S. 38f; *Gusy,* Aus Politik und Zeitgeschichte 2004, S. 20; *Gusy,* ZRP 2012, S. 233; *Graulich,* in: Graulich/Simon, S. 160. Dieses Defizit führt oftmals dazu, dass die politischen Gremien erst durch die Medien über etwaige Missstände informiert werden. *Huber,* NJW 2007, S. 881, spricht von einem „blinden Wächter ohne Schwert".

Verhältnis zu den Kontrollinstanzen suboptimal.[515] Aus diesem Grund wird zum Teil eine rechtliche und personelle Stärkung des PKGr beziehungsweise der ihm zuarbeitenden Einheiten gefordert.[516]

(2) G10-Kommission

Im Anwendungsbereich des G10 wird die nachträgliche Kontrolle durch die G10-Kommission ergänzt. Im Gegensatz zum PKGr führt die G10-Kommission keine politische, sondern eine begleitende, einzelfallbezogene Kontrolle durch.[517] Sie kontrolliert den gesamten Prozess der Informationserhebung, -verarbeitung und -nutzung auf Zulässigkeit und Notwendigkeit. Sie muss dementsprechend selbst nach Abschluss einer Überwachungsmaßnahme über deren Verlauf und Ergebnisse informiert werden.[518] Ihre Kontrollbefugnisse richten sich, wie bereits im Vorfeld der Maßnahme, nach § 15 V 3 G10. Sie nimmt in diesem Zusammenhang Beschwerden von Bürgern entgegen, überwacht die Einhaltung der Mitteilungspflichten an den Betroffenen und entscheidet über etwaige Verweigerungs- und Rückstellungsgründe.[519]

(3) Gerichtliche Kontrolle

Darüber hinaus kann die Informationserhebung einer nachträglichen Rechtskontrolle durch die Gerichte zugeführt werden. Im Bereich der Nachrichtendienste kann der Betroffene die Rechtmäßigkeit einer Überwachung vor den Verwaltungsgerichten überprüfen lassen.[520] Im Vergleich dazu unterliegen repressive Maßnahmen der Strafverfolgungsbehörden nach § 23 EGGVG der Kontrolle durch die ordentlichen Gerichte.[521]

Im Bereich der Geheimdienste ist der individuelle Rechtsschutz allerdings aus tatsächlichen Gründen oftmals schwach. Faktische Voraussetzung für das Beschreiten des Rechtswegs ist zunächst die Kenntnis des Betroffenen von der Überwachungsmaßnahme. Hieran fehlt es regelmäßig, wenn die Dienste die nach § 9 III BVerfSchG oder § 12 G10 erforderliche Mitteilung an den Betroffenen über einen längeren Zeitraum zurückstellen und der Betroffene aufgrund der Heimlichkeit der Informationsbeschaffung keine Kenntnis von der Maßnahme hat. Dies ist

---

515 *Baier,* S. 63, kritisiert vor allem die primär politische Ausrichtung der Kontrolle.

516 Vgl. *Hörauf,* S. 367.

517 So *Baier,* S. 93; *Huber,* NJW 2001, S. 3301.

518 Vgl. § 15 V G10 sowie *Droste,* Handbuch, S. 350.

519 Vgl. §§ 12, 15 VII G10.

520 Vertiefend *Droste,* Handbuch, S. 602; *Rose-Stahl,* S. 166.

521 Vgl. OVG Münster, Beschl.vom 9.1.2012, Az: 5 E 251/11.

etwa beim Abhören von Telefongesprächen sowie dem Öffnen und Einsehen von Briefsendungen der Fall. Selbst bei sonstiger Kenntniserlangung hat der Betroffene oftmals keine Möglichkeit, weitere Informationen zu erlangen. Zwar stehen ihm nach § 15 I BVerfSchG, § 7 Satz 1 BNDG und § 9 MADG Auskunftsansprüche zu,[522] die Erfolgschancen eines solchen Auskunftsersuchens sind jedoch aufgrund besonderer Begründungserfordernisse und verschiedener Ablehnungsgründe relativ gering.[523] Im Auskunftsantrag muss der Betroffene beispielweise auf einen konkreten Sachverhalt hinweisen und ein qualifiziertes Interesse an der Auskunft darlegen.

Diese im Nachrichtendienstrecht bestehenden Einschränkungen wurden bislang weder vom BVerfG noch vom EGMR beanstandet.[524] Das Fehlen von Rechtsschutzmöglichkeiten sei vielmehr durch den langfristigen Zweck geheimdienstlicher Beobachtungen, den Methodenschutz und die Schutzbedürfnisse der Gesellschaft gerechtfertigt. Dem Betroffenen stehe kein uneingeschränktes Recht auf Bekanntgabe von Überwachungsmaßnahmen zu. Eine bedenkliche Schwelle sei erst erreicht, wenn der Betroffene den durch die Heimlichkeit bedingten Informationsvorsprung in einem späteren Verfahren nicht mehr ausgleichen könne und hierdurch das Verfahren in seiner Gesamtheit als unfair zu betrachten sei.[525] Die Wahrnehmung der Rechtsschutzmöglichkeiten ist nach dieser Rechtsprechung letztlich von einer Gesamtabwägung abhängig.

Im Ergebnis sind im Geheimdienstsektor sowohl der Zugang zu den Gerichten als auch die Kontrolle vor den Gerichten erheblichen Einschränkungen unterworfen. Ein Großteil der Rechtsprechung befasst sich dementsprechend erst gar nicht mit der Rechtmäßigkeit geheimdienstlicher Maßnahmen, sondern beschränkt sich auf die Zugangsmöglichkeiten zu entsprechenden Informationen.[526]

dd) Zwischenergebnis zu Kontrollinstanzen

Die Tätigkeit der Nachrichtendienste wird von verschiedenen Organen kontrolliert. Anders als im Strafverfolgungssektor spielen dort neben den klassischen Kontrollinstanzen vor allem das PKGr und die G10-Kommission eine wichtige Rolle. Mit Ausnahme der Telekommunikationsüberwachung sind zudem die richterlichen Kontrollen der Nachrichtendienste im Vorfeld und im Anschluss an eine Informationserhebung rechtlich wie faktisch stärker eingeschränkt als im Strafverfolgungsbereich.

---

522 Vgl. auch *Baier,* S. 63.

523 Zur den geringen Erfolgschancen vgl. *Gusy,* Grundrechte, S. 86f, 103.

524 Zur entsprechenden Rechtfertigung vgl. EGMR NJW 1979, S. 1755ff.

525 Allgemein zur Heimlichkeit im Ermittlungsverfahren *Zöller,* StraFo 2008, S. 17.

526 Vgl. *Gusy,* Grundrechte, S. 87.

g) Zwischenergebnis zu den Besonderheiten geheimdienstlicher Ermittlungen

In den vorangegangenen Abschnitten wurden die Besonderheiten geheimdienstlicher Ermittlungen herausgearbeitet. Hierbei wurden unter anderem die nachrichtendienstlichen Aufgaben, Ermittlungsschwellen, Befugnisse und Kontrollinstanzen dargestellt. Es konnten vermehrt Überschneidungsbereiche zum Strafverfolgungs- und Polizeisektor nachgewiesen werden.[527] Die nachrichtendienstlichen Ermittlungsmethoden unterscheiden sich nur noch geringfügig von den Befugnissen anderer Sicherheitsbehörden.[528] Selbst in zeitlicher Hinsicht erfolgt eine zunehmende Verlagerung ins Vorfeld und damit eine gegenseitige Annäherung von Strafverfolgungs-, Polizei und Nachrichtendienstsektor[529] Allerdings können die Nachrichtendienste weiterhin leichter, umfassender und langfristiger Informationen erheben als die Strafverfolgungs- und Polizeibehörden.[530] Sie sind in der deutschen Sicherheitsarchitektur eine der wenigen staatlichen Behörden, die im Wege der strategischen Kontrolle anlasslose, einzelfallunabhängige und flächendeckende Beobachtungsmaßnahmen durchführen können. Zudem sind Aufgaben und Ziele der Nachrichtendienste, trotz diverser Annäherungstendenzen, keineswegs deckungsgleich zu denen anderer Sicherheitsbehörden.[531] Grundsätzlich dürfen geheimdienstliche Beobachtungsmaßnahmen nicht zur Aufklärung lediglich geringfügiger Sachverhalte, sondern nur zum Schutz hochrangiger Gemeinschaftsgüter eingesetzt werden.[532] Bei der Erfüllung dieses Beobachtungsauftrags bleiben ihnen aufgrund der Vorgaben des Trennungsgebots Zwangsbefugnisse allerdings verwehrt. Die Charakteristika nachrichtendienstlicher Überwachungsmaßnahmen zeigen sich letztlich weniger anhand von Spezialbefugnissen, sondern in Bezug auf die jeweils geltenden Anwendungsvoraussetzungen und der zulässigen Erhebungsbreite. Diese Besonderheiten sind zu einem erheblichen Anteil der Konzeption der Nachrichtendienste als staatliches Frühwarnsystem geschuldet. Die hierzu erforderliche strategische und langfristige Vorfeldbeobachtung wird aufgrund der Vorgaben des Trennungsgebots akzeptiert. Kommt es jedoch zu einem Austausch mit dem Strafverfolgungssektor, können gerade diese Spezifika einer Nutzung entgegenstehen. Die herausgearbeiteten Aspekte setzen insofern der Übermittlung und der Verwertung Grenzen, welche nachfolgend präzisiert werden.

---

527 Vgl. *Gusy,* ZRP 2008, S. 39.

528 Stellvertretend für viele *Gusy,* StV 1995, S. 325.

529 Vgl. *Wolff,* S. 7.

530 Vgl. *Droste,* Handbuch, S. 299; *Frister,* FS für Bemmann, S. 549; *Grawe,* S. 125; *Roggan,* in: Roggan/Kutscha, S. 415.

531 So *Singer,* OK, S. 295.

532 Vgl. *Engelhart,* in: Wade/Maljević, S. 514.

2. Allgemeine Grenzen einer Informationsnutzung

Der Nutzung von Geheimdienstinformationen sind allgemeine Grenzen gesetzt, deren Verlauf durch die Gestaltung der Rechts- und Sicherheitsarchitektur bestimmt werden.

a) Grenzen aufgrund der Sicherheitsarchitektur

Das Geheimdienstwesen wird maßgeblich durch die Gestaltungsvorgaben des Trennungsgebots bestimmt. Die befugnisrechtliche und organisationsrechtliche Dimension des Trennungsgebots wurde vom Gesetzgeber in den Nachrichtendienstgesetzen einfachgesetzlich geregelt.[533] Im Gegensatz dazu wurde die Zusammenarbeit durch den Polizeibrief keinen konkreten Vorgaben unterworfen. Dennoch wird dem Trennungsgebot zusätzlich zu den bereits beschriebenen Elementen eine informationelle Dimension zugesprochen.[534] Diese Komponente wurde zuletzt im Urteil des Bundesverfassungsgerichts vom 24.4.2013 zur ATD hervorgehoben.[535] Danach darf die Trennung nicht durch einen permanenten und vollumfänglichen Informationsaustausch umgangen werden. Die Ausübung polizeilicher Befugnisse durch die Nachrichtendienste wäre letztlich nicht mehr erforderlich, wenn die Beteiligten über den Informationsaustausch bereits Zugriff auf sämtliche Informationen hätten, da sie dann faktisch eine funktionale Einheit bilden würden.

Die informationelle Komponente des Trennungsgebots führt jedoch nicht dazu, dass ein Informationsaustausch per se unzulässig ist.[536] Eindeutig gestalten sich insofern die äußeren Grenzen eines Informationsaustausches. Danach sind sowohl ein schrankenloser Erkenntnisaustausch als auch ein absolutes Übermittlungsverbot mit den Vorgaben des Trennungsgebots unvereinbar.[537] Ein vollständiges Übermittlungsverbot würde weder dem Sinn noch dem historischen Hintergrund des Trennungsgebots gerecht werden. Die Alliierten wollten durch die Vorgaben des Polizeibriefs primär eine Vereinigung polizeilicher und geheimdienstlicher Befugnisse nach dem Vorbild der Gestapo für die Zukunft ausschließen. Gleichzeitig

---

533 Vgl. zur befugnisrechtlichen Trennung § 8 III BVerfSchG, § 2 III 1 BNDG, § 4 II MADG; zur organisatorischen Trennung § 2 I BVerfSchG, § 1 I 2 BNDG, § 1 IV MADG.

534 Zum Beispiel von *Baumann,* DVBl 2005, S. 798ff; *Klee,* S. 132f*; Kutscha,* in: Roggan/Kutscha, S. 81; *Kutscha,* NVwZ 2013, S. 324; *Pawlik,* JZ 2010, S. 696; *Roggan/Bergemann,* NJW 2007, S. 876; *Schünemann,* NStZ 2008, S. 306; *Singer,* Die Kriminalpolizei 2006, S. 88f.

535 Vgl. BVerfG, 1 BvR 1215/07, 1. Leitsatz, sowie Rn. 123.

536 Vgl. insgesamt *Engelhart,* in: Wade/Maljević, S. 509; *Gusy*, ZRP 2012, S. 232; *Klee,* S. 133; *Korte,* in: Korte/Zoller, S. 59; *Roggan/Bergemann,* NJW 2007, S. 876f; *Zöller,* in: Roggan/Kutscha, S. 465.

537 So auch *Baumann,* DVBl 2005, S. 800f; *Singer,* OK, S. 322.

sollte das deutsche Nachrichtendienstwesen, auch aus einem Eigeninteresse heraus, handlungsfähig sein. Mangels eigener Handlungsbefugnisse waren die deutschen Nachrichtendienste nach dem Plan der alliierten Streitkräfte von vorneherein auf eine Kooperation mit anderen Behörden angewiesen.[538] Ein vollständiger Ausschluss der Zusammenarbeit war dementsprechend zu keiner Zeit beabsichtigt.[539] Diese Erkenntnis wird durch die grundsätzliche Zielsetzung des Trennungsgebots bestätigt. Eine limitierte Übermittlung führt danach weder zu einer Anmaßung polizeilicher Befugnisse noch zu einer gestapoähnlichen Machtballung. Umgekehrt ist der gezielte und planmäßige Einsatz geheimdienstlicher Befugnisse zur Erlangung strafrechtlich relevanter Erkenntnisse unzulässig.[540] Das in diesem Zusammenhang maßgebliche Missbrauchsargument gilt sowohl für die Dienste als auch für die mit ihnen zusammenarbeitenden Behörden. Im vorliegenden Kontext dürfen die Dienste weder zur Umgehung polizeilicher und strafprozessualer Vorschriften instrumentalisiert werden noch sollen sich die Dienste durch die Informationsübermittlungen einen faktischen Vollzugsarm schaffen dürfen.[541] Zum Teil sind derartige Umgehungsverbote ausdrücklich in den heutigen Nachrichtendienstgesetzen vorgesehen.[542] Insgesamt soll verhindert werden, dass die Dienste repressive Aufgaben wahrnehmen, ohne selbst an die Vorgaben der Strafprozessordnung gebunden zu sein.[543] Eine Übermittlung von Geheimdienstinformationen darf insofern nicht die durch die Strafprozessordnung gesetzten Grenzen unterlaufen.[544]

An einer solchen bewussten Umgehung fehlt es bei der Übermittlung sogenannter Zufallsfunde. Hierbei handelt es sich um Erkenntnisse, die bei einer rechtmäßigen Überwachung „zufällig" anfallen, da deren Erlangung weder Anlass war noch

---

538 So Borgs-Maciejewski/Ebert-*Borgs*, § 3 BVerfSchG Rn. 30, 132ff.

539 Vgl. stellvertretend *Baumann,* DVBl 2005, S. 800f; *Droste,* Handbuch, S. 296; *Klee,* S. 133.

540 Vgl. MüKo StGB-*Lampe/Hegmann,* Vor §§ 93 ff Rn. 34; *Rogall,* ZStW 103 (1991), S. 942. Ebenfalls für die Eignungsprüfung *Schneider,* NJW 1978, S. 1602. Zum Verbot der gezielten Suche wegen Verantwortung der Staatsanwaltschaft vgl. *Schäfer/Wache/Meiborg,* Rn. 354.

541 Vgl. *Zöller,* in: Roggan/Kutscha, S. 499.

542 Vgl. § 8 III 2. Halbsatz BVerfSchG, § 2 III 2 BNDG; § 4 II 2. Halbsatz MADG. Vertiefend *Singer,* OK, S. 323.

543 Vgl. zur Umgehungsproblematik *Frister,* FS für Bemmann, S. 552; *Roggan,* in: Roggan/Kutscha, S. 421; *Singer,* OK, S. 58; *Singer,* Die Kriminalpolizei 2006, S. 88f; *Zöller,* JZ 2007, S. 767. Die Strafverfolgungsbefugnisse sind ausschließlich in der StPO benannt. Jede Behörde, die gezielt repressiv tätig wird, ist an die dort genannten Vorgaben gebunden.

544 So BT-Drs. 14/5655, S. 20. Diese Bindung wird vor allem in Bezug auf im Ausland erhobene Daten deutlich. Während dem BND die Informationserhebung im Ausland gestattet ist, sind die Strafverfolgungsbehörden an die Grenzen der Rechtshilfe gebunden. Für Geheimdienstinformationen aus Beobachtungsmaßnahmen im Ausland besteht damit grundsätzlich eine Übermittlungssperre, siehe hierzu *Schünemann,* NStZ 2008, S. 306.

sonst beabsichtigt wurde.[545] Wesentliches Merkmal eines Zufallsfundes ist neben dem Element der Zufälligkeit die Rechtmäßigkeit der ursprünglichen Informationserhebung.[546] Klassischerweise wird das Konstrukt des Zufallsfundes im strafrechtlichen Kontext verwendet.[547] Allerdings können Zufallsfunde auch im außerstrafprozessualen Rahmen vorkommen.[548] Der Beobachtungsauftrag der Nachrichtendienste richtet sich zwar auf staatsgefährdende Bedrohungen, aufgrund der umfassenden Erhebungsbreite lässt sich jedoch nicht ausschließen, dass in diesem Zusammenhang strafrechtlich relevante Erkenntnisse anfallen.[549] Geheimdienstliche Zufallsfunde können daher unter bestimmten Voraussetzungen ohne Verstoß gegen das Trennungsgebot übermittelt werden.[550] In den Nachrichtendienstgesetzen und dem G10-Gesetz finden sich zahlreiche Übermittlungsregelungen, die unter anderem die Informationsweitergabe an die Strafverfolgungsbehörden regeln. Eine dem Trennungsgebot zuwiderlaufende Informationsübermittlung soll vor allem durch Übermittlungsschwellen verhindert werden. Die Notwendigkeit solcher Übermittlungsschwellen wurde vom Bundesverfassungsgericht in Bezug auf die Fernmeldeüberwachung durch den BND festgestellt und hat allgemeine Geltung.[551] Insgesamt wird damit die Nutzung von Geheimdienstinformationen durch die Vorgaben des Trennungsgebots eingegrenzt, ein vollständiger Ausschluss ist damit jedoch nicht verbunden. Die konkrete Ausgestaltung der Übermittlungsmöglichkeiten richtet sich nach verfassungsrechtlichen Vorgaben. Diese sind unter anderem Gegenstand des nächsten Abschnitts.

---

[545] So u.a. der BGH in BGHSt 28, 122, 125, der Zufallsfunde als „bei einer zulässig angeordneten Überwachung gewonnene zufällige Erkenntnisse" definiert.

[546] Vgl. hierzu *Droste,* Handbuch, S. 475; *Grawe,* S. 151; *Rogall,* JZ 1996, S. 949. Grawe bezeichnet den Begriff des rechtswidrigen Zufallsfundes sogar als Oxymoron. Sinngemäß auch *Forkert-Hosser,* S. 293f; *Lohberger,* FS für Hanack, S. 259; *Zöller,* in: Roggan/Kutscha, S. 499. Zur Definition des Zufallsfundes vgl. *Grawe,* S. 142f; *Schwörer,* S. 117ff. Letzterer verweist auf die Definitionsschwierigkeiten der Rechtsprechung. Zur Unzulässigkeit der gezielten Suche nach „Zufallsfunden" *Roggan/Bergemann,* NJW 2007, S. 876; *Zöller,* in: Roggan/Kutscha, S. 465.

[547] Vgl. *Allgayer/Klein,* wistra 2010, S. 130; *Lohberger,* FS für Hanack, S. 261; *Rogall,* ZStW 103 (1991), S. 942.

[548] Vgl. *Grawe,* S. 124f, 175f, 279. Ablehnend zum Begriff des Zufallsfundes im Nachrichtendienstsektor *Rehbein,* S. 209. Diese knüpft das Vorliegen eines Zufallsfundes vor allem an das Merkmal des Verdachts. Da dieser bei nachrichtendienstlichen Ermittlungen regelmäßig nicht oder nur gering ausgebildet sei, scheide ein Zufallsfund aus.

[549] Allerdings gibt es bestimmte geheimdienstliche Ermächtigungsgrundlagen, bei denen eine korrekte Durchführung erst gar nicht oder nicht in wenigen Fällen zu einem Zufallsfund kommen sollte. Dies ist beispielsweise bei der strategischen Telekommunikationsüberwachung der Fall, die gerade mit ausgewählten Stichworten arbeitet.

[550] BVerfG NJW 2000, S. 55ff; *Engelhart,* in: Wade/Maljević, S. 507; Wabnitz/Janovsky-*Tschanett*, Handbuch, 29. Kapitel, II. unter 13. Nachrichtendienste, Rn. 27. Für eine auf Zufallsfunde limitierte Übermittlung *Huber,* NJW 2001, S. 3300; *Zöller,* in: Roggan/Kutscha, S. 499.

[551] So BVerfG NJW 2000, S. 55, 66, unter Bezugnahme auf die Schwelle des § 100a StPO; vgl. zudem *Schünemann,* NStZ 2008, S. 306.

b) Grenze aufgrund der Rechte des Betroffenen

Weitere Grenzen einer Informationsnutzung ergeben sich aus den Rechten der Betroffenen und dabei insbesondere aus den Grundrechten. Die mit einer Informationsnutzung verbundenen Grundrechtseingriffe unterliegen allgemeinen verfassungsrechtlichen Grenzen, die auch bei der Nutzung von Geheimdienstinformationen zu beachten sind. In Betracht kommen Eingriffe in das Recht auf informationelle Selbstbestimmung, das Brief-, Post- und Fernmeldegeheimnis, die Unverletzlichkeit der Wohnung sowie die übrigen Bereiche des allgemeinen Persönlichkeitsrechts.[552] Darüber hinaus kann die Informationserhebung die Glaubens-, Gewissens- und Bekenntnisfreiheit, das Recht der freien Meinungsäußerung, den Schutz von Ehe und Familie, die Versammlungsfreiheit und die Berufsfreiheit betreffen.

Die nachrichtendienstliche Informationserhebung erfasst unter anderem die Sammlung personenbezogener Daten.[553] Dementsprechend muss sich die Nutzung von Geheimdienstinformationen auch und vor allem am Recht auf informationelle Selbstbestimmung messen lassen.[554] Dieses gewährleistet den Schutz des Einzelnen vor der unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Daneben verbürgt es das Recht, selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen zu können.[555] Die durch die Grundrechte gesetzten Grenzen werden stellvertretend am Recht auf informationelle Selbstbestimmung dargestellt. In dieses kann sowohl durch die Erhebung und Speicherung als auch die Weitergabe der Informationen eingegriffen werden.[556] Bei der nachrichtendienstlichen Informationsgewinnung erfolgt der erste Grundrechtseingriff durch die Informationserhebung selbst, welche die Information aus ihrem privaten Kontext löst. Die Speicherung setzt diesen Eingriff fort, indem die staat-

---

[552] Das Brief-, Post- und Fernmeldegeheimnis schützt die Vertraulichkeit des durch Kommunikationsmittel unterstützten individuellen Informationsaustausches, für dessen Zustandekommen zunächst eine gewisse Distanz überwunden werden muss. Geschützt werden Inhalt und Umstände der Kommunikation in ihrer Freiheit und Privatheit, vgl. BVerfGE 85, 386, 395, sowie Epping/Hillgruber-*Baldus,* Art. 10 Rn. 1; *Bertram,* S. 78. Die Unverletzlichkeit der Wohnung verbürgt demgegenüber den räumlich-gegenständlichen Bereich der Privatsphäre, der der Entfaltung der Persönlichkeit dient, vgl. BVerfGE 989, 1, 12; *Bertram,* S. 81; Maunz/Dürig-*Papier,* Art. 13 Rn. 1.

[553] Vgl. § 3 I BVerfSchG, § 2 I BNDG. Bei diesen Daten handelt es sich um „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person", § 3 I BDSG. Für den Personenbezug genügt, wenn sich die Zuordnung aus dem Inhalt der Angaben oder unter Rückgriff auf weitere verfügbare Erkenntnisse ergibt; vgl. *Gola/Schomerus,* BDSG, § 3 Rn. 10.

[554] Dieser Überschneidungsbereich wird auch als grundrechtlicher Datenschutz bezeichnet, vgl. BVerfG NJW 1991, S. 2129, 2132. Vertiefend zur Lehre vom informationellen Selbstbestimmungsrecht *Rogall,* ZStW 103 (1991), S. 919ff.

[555] Vgl. BVerfGE 65, 1, 42, sowie 1. Leitsatz.

[556] Vgl. zu den verschiedenen Informationseingriffen *Gusy,* NVwZ 1983, S. 324ff. Zu den Belastungen einer bloßen Weitergabe vgl. bereits *Schneider,* NJW 1978, S. 1603.

liche Teilhabe perpetuiert und die Vervielfältigung und Weitergabe ermöglicht wird.[557] Durch die Übermittlung kommt es zu einem dritten Grundrechtseingriff.[558] Durch diese werden die Informationen einem neuen Teilnehmerkreis zur Verfügung gestellt. In diesem neuen Verwendungszusammenhang ist für den Einzelnen nicht mehr überschaubar, wer zu welchen Zwecken auf die Informationen zugreifen kann.[559] Neben der Erweiterung des Personenkreises ist hierbei vor allem von Interesse, *wem* die Informationen konkret zur Verfügung gestellt werden.[560] Die Übermittlung von Geheimdienstinformationen an die Strafverfolgungsbehörden kann für den Einzelnen mit erheblichen persönlichen Konsequenzen verbunden sein.

Diese Grundrechtseingriffe können allerdings unter Einhaltung bestimmter Vorgaben gerechtfertigt werden. Grundlegende Voraussetzung ist zunächst das Vorliegen einer Ermächtigungsgrundlage. Diese Vorgabe entspringt dem sogenannten Vorbehalt des Gesetzes, der überwiegend als Verfassungsprinzip anerkannt und dem Rechtsstaats- und Demokratieprinzip entnommen wird.[561] Bei wesentlichen Grundrechtseingriffen verdichtet sich der Gesetzesvorbehalt zum Parlamentsvorbehalt, demzufolge das Parlament alle wesentlichen, die Allgemeinheit betreffenden Fragen selbst klären und regeln muss.[562] Bei einer Informationsübermittlung müssen entsprechende Ermächtigungen sowohl aufseiten der Übermittlungs- als auch der Empfangsbehörde vorliegen. Die Notwendigkeit korrespondierender Ermächtigungen wird als Modell der doppelten Tür bezeichnet (siehe Abb. 2, S. 106) und wurde zuletzt durch einen Beschluss des Bundesverfassungsgerichts im Jahr 2012 bestätigt.[563] Danach fällt das Ob der Übermittlung in die Gesetzgebungskompetenz des Primärgesetzgebers und ist damit in den Nachrichtendienstgesetzen zu regeln. Die strafprozessuale Nutzung fällt demgegenüber in die Gesetzgebungskompetenz der Empfangsbehörden und ist folglich in der StPO zu regeln.[564] Die notwendigen

---

[557] Nach § 3 IV 1 Nr. 1 BDSG wird u.a. das Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung erfasst. Vertiefend zu den Gefahren der Datenverarbeitung vgl. BVerfGE 65, 1, 42 sowie *Rogall,* ZStW 103 (1991), S. 928, 930.

[558] Nach § 3 IV 1 Nr. 4 BDSG versteht man unter einer Übermittlung die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten. Vgl. zur Grundrechtsrelevanz BVerfG NJW 2000, S. 55, 65; *Rogall,* ZStW 103 (1991), S. 930.

[559] Vgl. BVerfGE 65, 1, 43; *Bertram,* S. 36; *Ernst,* S. 71ff; *Kretschmer,* JURA 2006, S. 439; *Simitis,* NJW 1984, S. 399.

[560] Vgl. *Rogall,* ZStW 103 (1991), S. 928.

[561] Vgl. *Bertram,* S. 78.

[562] Vgl. *Zöller,* in: Roggan/Kutscha, S. 454f. Vertiefend *Maurer,* § 6 Rn. 6ff.

[563] Siehe den Beschluss des BVerfG vom 24.2.2012, 1 BvR 1299/05.

[564] Vgl. *Singelnstein,* ZStW 120 (2008), S. 863, 878. Zu den verschiedenen Modellen vgl. *Bertram,* S. 308ff; *König,* S. 289; *Paeffgen,* FS für Hilger, S. 155f; *Zöller,* Handbuch, S. 461.

Ermächtigungsgrundlagen müssen einen legitimen Gemeinwohlzweck verfolgen sowie dem Gebot der Normenklarheit und dem Verhältnismäßigkeitsprinzip genügen.[565]

Im Bereich personenbezogener Daten wird das Verhältnismäßigkeitsprinzip durch den Zweckbindungsgrundsatz präzisiert. Dieser Grundsatz besagt zweierlei: Zum einen müssen personenbezogene Daten zweckgebunden erhoben werden. Zum anderen sind diese Daten bei der weiteren Verwendung grundsätzlich an diesen ursprünglichen Erhebungszweck gebunden.[566] Die Erweiterung des ursprünglichen Nutzungszwecks durch eine Übermittlung an andere Sicherheitsbehörden kann daher unverhältnismäßig sein. Die Bedeutung des Zweckbindungsgrundsatzes wird vor allem bei einer Übermittlung von Geheimdienstinformationen an den Strafverfolgungssektor deutlich. Dort wird die ursprünglich zu präventiven Zwecken erhobene Information einer repressiven Nutzung zugeführt. Der Informationstransfer ist damit nicht nur mit einer quantitativen, sondern sogar mit einer qualitativen Zweckverschiebung verbunden. Der Zweckbindungsgrundsatz steht einer Übermittlung und damit Zweckänderung jedoch nicht vollends entgegen. Vielmehr ist die Zweckänderung mit einem Grundrechtseingriff verbunden, der unter bestimmten Voraussetzungen gerechtfertigt werden kann. Zu differenzieren ist zwischen internen und externen Vorgängen. Innerhalb des Geheimdienstsektors wird der Zweckbindungsgrundsatz durch die Nachrichtendienstgesetze ausdrücklich ausgeschlossen.[567] Da den Geheimdiensten ein umfassender Beobachtungsauftrag obliegt, müssen sie in der Lage sein, die einzelnen erhobenen „Mosaiksteine" zu speichern und zusammenzusetzen.[568] Bei einer Übermittlung an externe Behörden kommt der Grundsatz der Zweckbindung wiederum uneingeschränkt zur Anwendung. Bei einer Übermittlung von Geheimdienstinformationen an den Strafverfolgungssektor müssen daher neben dem Merkmal des Zufallsfundes zusätzlich die Voraussetzungen des Zweckbindungsprinzips beachtet werden.

Eine Verletzung des Zweckbindungsgrundsatzes kann durch eine Einwilligung des Betroffenen oder eine legitime Zweckänderung verhindert werden.

Die Einwilligung des Betroffenen nach § 183 BGB, § 4a I BDSG muss auf einer freien und informierten Entscheidung des Betroffenen beruhen und in Schriftform erteilt werden. Unabhängig davon, ob man die Einwilligung als Grundrechtsausübung, Grundrechtsverzicht oder Rechtfertigung des Grundrechtseingriffs qualifiziert, verhindert diese zumindest eine Grundrechts*verletzung*, wenn nicht sogar

---

565 BVerfG NJW 2000, S. 55, 57.

566 Vgl. BVerfGE 65, 1, 46; *Bertram,* S. 138.

567 In diesem Sinne schließen die Nachrichtendienstgesetze die Anwendung des § 14 BDSG ausdrücklich aus; vgl. auch *Bäumler,* NVwZ 1991, S. 644.

568 So *Wolff,* S. 159. Dies ergibt sich bereits im Umkehrschluss aus § 9 II 10 BVerfSchG, der nur ausnahmsweise eine Zweckbindung vorsieht.

einen Eingriff in den Schutzbereich als solchen.[569] Letztlich soll der Grundrechtsträger nur vor Verarbeitungsvorgängen geschützt werden, die gegen oder ohne seinen Willen erfolgen.[570] Die datenschutzrechtlichen Regeln sind insofern als Verbot mit Erlaubnisvorbehalt ausgestaltet.[571] Diese Einwilligungsvariante wird im Geheimdienstsektor allerdings bereits aus Quellen- und Selbstschutzgründen kaum zur Anwendung kommen, da die Dienste im besonderen Maße auf eine möglichst langfristige Geheimhaltung ihrer Beobachtungsmaßnahmen angewiesen sind.[572] Selbst bei einer Offenbarung der Dienste gegenüber dem Betroffenen wird dieser einer Übermittlung an die Strafverfolgungsbehörden aufgrund der damit verbundenen Gefahr einer Strafverfolgung nur in wenigen Fällen zustimmen.

Liegt keine Einwilligung vor, müssen die von der Rechtsprechung aufgestellten Voraussetzungen einer nachträglichen Zweckänderung erfüllt sein.[573] Diese erfordert im Einzelnen (1.) das Bestehen einer formell und materiell verfassungsgemäßen gesetzlichen Grundlage, (2.) die Rechtfertigung der Zweckänderung durch überwiegende Allgemeinbelange,[574] (3.) einen Bezug zu den Aufgaben und Befugnissen der Empfangsbehörde sowie (4.) die Vereinbarkeit des Erhebungs- mit dem künftigen Verwendungszweck. Schließlich muss (5.) die Verhältnismäßigkeit der Übermittlung als solche gewahrt sein.[575] Das Merkmal der Vereinbarkeit von Erhebungs- und Verwendungszweck soll sicherstellen, dass der Empfangsbehörde nur solche Informationen übermittelt werden, die sie selbst hätte erheben dürfen.[576] Bei einer Übermittlung von dem Geheimdienst- an den Strafverfolgungssektor wäre von einer Unvereinbarkeit auszugehen, wenn durch die Zweckänderung Voraussetzungen der Strafprozessordnung umgangen würden und die Strafverfolgungsbehörden die übermittelten Informationen für eigene Zwecke nicht oder nicht in dieser Art und Weise hätten erheben dürfen.[577]

---

569 Für eine Einwilligung vgl. u.a. *Geiger,* NVwZ 1989, S. 37. Für einen Verzicht vgl. *Zöller,* in: Roggan/Kutscha, S. 455. Insgesamt vertiefend *Robbers,* JuS 1985, S. 925ff.

570 Vgl. *Geiger,* NVwZ 1989, S. 37.

571 Dieser Grundsatz kommt insbesondere in § 4 I BDSG zum Ausdruck, vgl. *Zöller,* in: Roggan/Kutscha, S. 456.

572 Vgl. *Zöller,* in: Roggan/Kutscha, S. 456.

573 Vgl. zu den Anforderungen an die Zweckänderung BVerfG NJW 1984, S. 419; BVerfG NJW 2006, S. 1939, 1946; BVerfG NJW 2008, S. 2135, 2138.

574 BVerfG, NJW 1984, 419, 2. Leitsatz. Dieser Prüfungspunkt entspricht der legitimen Zwecksetzung im Rahmen der klassischen Verhältnismäßigkeitsprüfung.

575 Hierzu eingehend BVerfG NJW 2000, S. 55ff.

576 Vgl. SächsVerfGH NVwZ 2005, S. 1310, 1315. Allgemein MüKoStGB-*Lampe/Hegmann,* Vor §§ 93 ff Rn. 34; *Rogall,* ZStW 103 (1991), S. 942.

577 Vgl. SächsVerfGH NVwZ 2005, S. 1310, 1315, mit Verweis auf BVerfG NJW 1984, S. 419, 322, zur Zweckentfremdung sowie BVerfG NJW 2000, S. 55, 57, zu den Anforderungen der Zweckänderung.

Wann eine Unvereinbarkeit gegeben ist, bestimmt sich damit im Einzelfall anhand der jeweiligen Parallelnormen.[578]

Die Verhältnismäßigkeit einer Übermittlungsregelung richtet sich wiederum nach der Intensität der Erhebungsmethode, dem späteren Verwendungszusammenhang sowie Art und Umfang der erhobenen Daten.[579] Der Verwendungszusammenhang betrifft die Frage, zu welchen und zu wie vielen Zwecken die Informationen im Rahmen der Sekundärnutzung zugänglich gemacht werden.[580] Werden Geheimdienstinformationen in einen außergeheimdienstlichen Kontext übermittelt, erhöhen sich die an die Angemessenheit der Übermittlungsregelungen zu stellenden Anforderungen.[581] Hierbei müssen im Einzelnen berücksichtigt werden: (1.) die ursprünglichen Erhebungsgrenzen beziehungsweise Handlungsschwellen, (2.) die für die Übermittlung erforderliche Tatsachenbasis, das heißt die sogenannten Übermittlungsschwellen sowie (3.) die durch die Übermittlung bezwecken Belange.[582] Da die Handlungsschwellen im Geheimdienstsektor sehr niedrig angesetzt sind, wird die Angemessenheit der nachrichtendienstlichen Übermittlungsregeln durch erhöhte Anforderungen an die zwei letztgenannten Kriterien kompensiert. Eine Übermittlung vonseiten der Geheimdienste scheidet damit regelmäßig bei Fällen minderschwerer Kriminalität oder bei einer zu geringen Tatsachenbasis aus. Die durch die Übermittlung verfolgten Belange müssen das durch den Informationseingriff betroffene Grundrecht überragen.[583] Ein überwiegendes Strafverfolgungsinteressen wird man bei einer Verletzung gewichtiger Rechtsgüter oder schweren Straftaten bejahen können.[584] Die Art des betroffenen Rechtsgutes beeinflusst zugleich die Höhe der Übermittlungsschwellen und damit die an die Übermittlung zu stellende Tatsachenbasis. Mit steigender Bedeutung des Rechtsgutes und zunehmender Schwere der Beeinträchtigung sinken grundsätzlich die an die Übermittlungsschwelle zu stellenden Anforderungen. Da im Bereich der Repression die Beeinträchtigung des Rechtsgutes allerdings nicht mehr verhindert werden kann, darf die erforderliche Tatsachenbasis nicht unter vergleichbare strafprozessu-

---

[578] Für den Bereich der Wohnraumüberwachung wurde in SächsVerfGH NVwZ 2005, S. 1310, 1315f, beispielweise ein Vergleich mit der Norm des § 100c StPO herangezogen. Es wurde die Unvereinbarkeit angenommen, da sich die Katalogstraftaten der Strafprozessordnung nicht mit denen des Landesverfassungsschutzgesetzes deckten.

[579] Neben der Übermittlung muss die ursprüngliche Erhebungsmaßnahme ebenfalls dem Verhältnismäßigkeitsgrundsatz genügen.

[580] Vgl. *Bertram,* S. 139f.

[581] Vgl. BVerfGE 65, 1, 46. Vertiefend zur Zweckänderung *Würtenberger/Heckmann,* Rn. 624ff. Nach *Schneider,* NJW 1978, S. 1603, handelt es sich bei den Übermittlungsregeln um einen vorverlegten Rechtsschutz.

[582] Zu diesen Kriterien BVerfG NJW 2000, S. 55, 66.

[583] Vgl. BVerfG NJW 2000, S. 55, 66.

[584] Vgl. BVerfG NJW 2000, S. 55, 66; *Grawe,* S. 126.

ale Schwellen abgesenkt werden.[585] Hierdurch wird die Zahl der tatsächlich an die Strafverfolgungsbehörden übermittelten Fälle minimiert.

Die Einräumung einer Übermittlungsbefugnis führt jedoch nicht automatisch zur strafprozessualen Verwertbarkeit dieser Erkenntnisse. Die Entscheidung über die Verwertbarkeit übermittelter Daten fällt vielmehr in den Regelungsbereich der Strafprozessordnung.[586] Die Übernahme von Geheimdienstinformationen zu Strafverfolgungszwecken stellt einen selbstständigen Eingriff in das Recht auf informationelle Selbstbestimmung dar und bedarf daher einer eigenständigen Ermächtigungsgrundlage in der Strafprozessordnung.[587] Die Zweckänderung ist damit sowohl bei der Übermittlung als auch bei der Entgegennahme der Informationen zu berücksichtigen. Bei einer Übermittlung durch die Landesämter für Verfassungsschutz ergibt sich dies außer aus der grundrechtlichen Relevanz auch aus der föderalen Struktur des deutschen Rechtssystems. Die jeweiligen Landesgesetzgeber sind über das Entlassen der Information hinaus nicht zur Regelung der weiteren strafprozessualen Verwendbarkeit befugt.[588] Diese fällt vielmehr in die Kompetenz des Bundes. Dementsprechend werden bei einer zweckändernden Nutzung die klassischen Verwertungsregeln durch sogenannte Verwendungsregeln ergänzt.[589] Letztere beziehen sich auf personenbezogene Daten und bestimmen das Ob und Wie einer zweckändernden Nutzung. Der Begriff der Nutzung ist dabei umfassend zu verstehen. Die Verwendungsregel ist nicht auf ein bestimmtes Verfahrensstadium fixiert, sondern kann im strafprozessualen Kontext sowohl die Nutzung der Information als Beweismittel als auch ihre Heranziehung als Spurenansatz begrenzen.[590] Verwertungsregeln beziehen sich dagegen lediglich auf einen Teilbereich der Verwendung. Sie legen fest, wann ein Beweismittel ausnahmsweise nicht in die Entscheidungsfindung einfließen darf. Im Gegensatz zu den Verwendungsregeln ist ihre Wirkkraft auf die strafprozessuale Phase der Hauptverhandlung schränkt. Dort können sie allerdings umfassend in Bezug auf alle personenbezogenen und nicht personenbezogenen Beweismittel zur Anwendung kommen. Bei der Nutzung von

---

[585] So *Engelhart,* in: Wade/Maljević, S. 516. Siehe das SächsVerfGH NVwZ 2005, S. 1310, 1315, für Eingriffe in Art. 13 GG unter Verweis auf die Schwere des Eingriffs. Siehe BVerfG NJW 2000, S. 55, 66, für Eingriffe in Art. 10 GG. Danach ist für Eingriffe nach §§ 1, 3 G10 die Schwelle des § 100a StPO als Leitlinie heranzuziehen.

[586] Vgl. *Bernsmann/Jansen,* StV 1998, S. 231; *Grawe,* S. 286; *Hefendehl,* StV 2001, S. 705f; *Singelnstein,* ZStW 120 (2008), S. 878 Fn. 118; *Welp,* NStZ 1995, S. 603.

[587] Vgl. *Singelnstein,* ZStW 120 (2008), S. 857, 864. Allgemein zur übertragbaren zweckändernden Übernahme präventiv-polizeilicher Informationen *Bertram,* S. 315. Zum Eingriffscharakter der Zweckänderung vgl. *Rehbein,* S. 143.

[588] Vgl. *Grawe,* S. 286.

[589] Vgl. *Rehbein,* S. 145ff, sowie allgemein *Singelnstein,* ZStW 120 (2008), S. 865ff. Letzterer kritisiert, dass der Gesetzgeber diese Differenzierung nicht immer sauber einhält.

[590] Vgl. *Rehbein,* S. 147f.

Geheimdienstinformationen im Strafprozess müssen folglich sowohl die Anforderungen der Verwendungs- als auch der Verwertungsregeln berücksichtigt werden. Chronologisch betrachtet beantworten die Verwendungsregeln damit die zeitlich vorgelagerte Frage, ob und inwieweit eine zweckändernde Übernahme von Geheimdienstinformationen rechtmäßig ist.[591] Im Anschluss daran klären die Verwertungsregeln, inwiefern die grundsätzlich verwendbaren Daten aufgrund eines Verwertungsverbots von der Beweiswürdigung ausgeschlossen werden müssen.

Die verfassungsrechtlichen Grenzen einer Informationsnutzung werden damit maßgeblich durch das Recht auf informationelle Selbstbestimmung sowie den daraus folgenden Zweckbindungsgrundsatz bestimmt. Werden die vorgenannten Voraussetzungen der Übermittlungs- und Empfangsnormen eingehalten, können Geheimdienstinformationen in verfassungskonformer Weise Eingang in ein Strafverfahren finden. Um die Einhaltung des Zweckbindungsprinzips überprüfen zu können, werden diese inhaltlichen Anforderungen zusätzlich durch verfahrensrechtliche Schutzvorkehrungen wie Aufklärungs-, Auskunfts-, Löschungs-, Kennzeichnungs- und Protokollierungsvorschriften ergänzt.[592]

c) Zwischenergebnis: Grenzen

Die vorangegangenen Ausführungen haben einen kurzen Einblick über die allgemeinen Grenzen einer Nutzung von Geheimdienstinformationen vermittelt. Dabei wurde deutlich, dass eine Zweckentfremdung in Form der Datenübermittlung zulässig sein kann. Von zentraler Bedeutung sind in diesem Zusammenhang das Trennungsgebot mit der Begrenzung auf Zufallsfunde sowie die Vorgaben des Zweckbindungsprinzips und der Zweckänderung. Wesentliche Grundsätze der Übermittlung und Verwendung von personenbezogenen Geheimdienstdaten wurden dabei von der Rechtsprechung entwickelt.[593] Diese Vorgaben haben zum Teil

---

[591] So *Singelnstein,* ZStW 120 (2008), S. 867. Bislang gehen die Gerichte von der grundsätzlichen Verwertbarkeit von Geheimdienstinformationen aus, vgl. etwa BGH StV 1990, S. 297 (Telefonüberwachung durch den Verfassungsschutz); KG Berlin StV 1995, 438 (Bericht eines Mitarbeiters des Verfassungsschutzes als Urkundsbeweis); BGH StV 2001, S. 216, 218; BGH StV 2001, S. 510, 514 (Telefonmitschnitte des Verfassungsschutzes); BGH StV 2001, S. 649f (Mitarbeiter des BfV als Zeuge).

[592] Vgl. *Singelnstein,* ZStW 120 (2008), S. 860. Vertiefend zur Zweckänderung BVerfGE 100, 313, 389f; 109, 279, 376f; 110, 33, 69f.

[593] Vgl. BT-Drs. 11/4306, S. 59. So wurden die heutigen Übermittlungsschwellen des G10 beispielsweise als Reaktion auf die Entscheidung des Bundesverfassungsgerichts zur Fernmeldeüberwachung vom 14. Juli 1999 geschaffen, vgl. BVerfGE 100, 313, 394. In diesem wurde die damalige Schwelle der tatsächlichen Anhaltspunkte als zu niedrig eingestuft; vgl. zudem BT-Drs. 14/5655, S. 21. Diese Grundsätze wurden durch Entscheidungen zum Großen Lauschangriff in BVerfGE 109, 279ff, sowie zur Überwachung nach dem Außenwirtschaftsgesetz in BVerfGE 110, 33ff, bestätigt und weiter konkretisiert.

Eingang in das Gesetz gefunden.[594] Die konkrete Ausgestaltung der Informationsübermittlung von den Nachrichtendiensten an die Strafverfolgungsbehörden ist Gegenstand des nachfolgenden Abschnitts.

3. Übermittlung von Geheimdienstinformationen

Die Übermittlung von Geheimdienstinformationen an die Strafverfolgungsbehörden kann auf Initiative der Dienste oder Anfrage der Strafverfolgungsbehörden erfolgen. Der umgekehrte Informationsfluss von Strafverfolgungsdaten an die Nachrichtendienste ist vorliegend nicht von Interesse.

a) Eigenständige Übermittlung durch die Dienste

Die sogenannte Spontan- beziehungsweise Eigeninitiativübermittlung vonseiten der Nachrichtendienste ist vor allem in den §§ 19, 20 BVerfSchG und den §§ 4, 7 G10 vorgesehen. Die dort aufgestellten Vorgaben gelten direkt beziehungsweise über die Verweisungsnormen der § 21 BVerfSchG, § 11 II MADG, § 9 III BNDG für das gesamte Nachrichtendienstwesen auf Bundes- und Landesebene.[595] Die Darstellung beschränkt sich daher auf die Regeln des BVerfSchG und des G10.

aa) Übermittlung nach § 20 BVerfSchG

Die zentrale Ermächtigungsgrundlage für eine Informationsübermittlung an die Strafverfolgungsbehörden findet sich in § 20 I 1 BVerfSchG. Diese Vorschrift begründet in Angelegenheiten des Staats- und Verfassungsschutzes eine Übermittlungspflicht, ohne dass es hierzu einer ausdrücklichen Aufforderung oder eines Auskunftsverlangens bedarf.[596]

Voraussetzung einer Übermittlung nach § 20 I 1 BVerfSchG sind „tatsächliche Anhaltspunkte", dass die Übermittlung zur Verhinderung oder Verfolgung von Staatsschutzdelikten „erforderlich" ist.[597] Die Annahme tatsächlicher Anhaltspunkte erfordert hinreichend konkrete Tatsachen und ist damit an die Schwelle des Anfangsverdachts i.S.d. § 152 II StPO angelehnt.[598] Bloße Vermutungen sind da-

---

[594] Für die geheimdienstliche Informationserhebung in §§ 8–9 BVerfSchG, für die Speicherung in §§ 10–11 BVerfSchG und für die Weitergabe in §§ 19ff BVerfSchG. Im Bereich der Verwendungsregeln kommt die Vorschrift des § 161 II StPO zur Anwendung.

[595] Teilweise existieren vergleichbare Regelungen für die LfV auch auf Landesebene.

[596] Vgl. *Griesbaum,* FS für Nehm, S. 134. Für die Landesverfassungsschutzbehörden findet sich die maßgebliche Regelung in § 21 BVerfSchG. Zu den Schwachstellen der Übermittlungsregelungen der LVerfSchG vgl. *Schäfer/Wache/Meiborg,* Rn. 348.

[597] Vgl. hierzu insgesamt *Zöller,* in: Roggan/Kutscha, S. 499ff.

[598] Vgl. *Zöller,* in: Roggan/Kutscha, S. 501, demzufolge eine vollumfängliche Überprüfung des Anfangsverdachts von den Diensten nicht gefordert werden kann.

mit nicht ausreichend, vielmehr müssen genügend Indizien vorhanden sein, die vor dem Hintergrund des nachrichtendienstlichen Erfahrungsschatzes für die Annahme eines Staatsschutzdeliktes ausreichen.[599] Die Tatsachen müssen sowohl auf die genannten Delikte hinweisen als auch für die Strafverfolgung notwendig sein.[600] Das Merkmal „zur Verfolgung von Straftaten erforderlich" i.S.d. § 20 I 1 BVerfSchG ist umfassend zu verstehen und beginnt bereits mit der Überprüfung des Anfangsverdachts.[601] Ein anhängiges Ermittlungsverfahren ist nicht gefordert. Der zweite Bezugspunkt der tauglichen Staatsschutzdelikte wird in § 20 I 2 BVerfSchG weiter präzisiert. Danach werden die Kataloge der §§ 74a, 120 GVG sowie sonstige Straftaten erfasst, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie sich gegen die in Art. 73 Nr. 10b, 10c GG normierten Schutzgüter richten.[602] Die letztgenannte Kategorie bezieht die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes sowie die auswärtigen Belange der Bundesrepublik Deutschland mit ein. Durch den Verweis auf die Grundrechtsnorm werden die Übermittlungsmöglichkeiten auf beinahe jede Straftat mit staatsschutzrechtlichem Bezug erweitert.[603] Ausgenommen sind Fälle einfacher Kriminalität sowie Delikte ohne staatsschutzrechtlichen Zusammenhang.[604] Trotz des schwerwiegenden Charakters eines Tötungsdeliktes wäre beispielsweise ein klassischer Eifersuchtsmord nicht erfasst, da der über die Einzelkriminalität hinausgehende Bezug zum Staatsschutz fehlt.

Zusätzlich zu den in § 20 I 1 BVerfSchG genannten Voraussetzungen sind die allgemeinen Übermittlungsgrenzen in den §§ 23ff BVerfSchG gegebenenfalls i.V.m. § 12 MADG, § 10 BNDG zu berücksichtigen.[605] Nach § 23 BVerfSchG unterbleibt eine Übermittlung, wenn die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an einer Übermittlung überwiegen (Nr. 1), überwiegende Sicherheitsinteressen ein Unterlassen der Übermittlung erfordern (Nr. 2) oder besondere gesetzliche Übermittlungsregelungen entgegenstehen (Nr. 3).[606] Daneben schränkt die Vorschrift des § 24 BVerfSchG die Übermittlung aus Gründen des Minderjährigenschutzes ein.[607]

---

[599] Vgl. *Zöller,* in: Roggan/Kutscha, S. 501.

[600] Vgl. *Droste,* Handbuch, S. 543.

[601] Vgl. *Griesbaum,* FS für Nehm, S. 132f.

[602] Vgl. *Wolff,* S. 131.

[603] So *Wolff,* S. 132, der daher eine restriktive Auslegung befürwortet.

[604] Zur Begrenzung auf Staatsschutzdelikte vgl. *Kühne,* Strafprozessrecht, Rn. 393.2. Dies geht bereits aus dem Gesetzestitel hervor.

[605] Schließlich kommen ergänzend die Grundsätze des BDSG zur Anwendung, sofern sie nicht nach § 27 BVerfSchG explizit ausgeschlossen sind.

[606] Eine eingehende Untersuchung dieses Übermittlungsverbots erfolgt im Rahmen der Geheimhaltungsproblematik.

[607] Vertiefend bei *Droste,* Handbuch, S. 555.

Stehen der Übermittlung keine Hindernisse entgegen, übermittelt der Verfassungsschutz nach § 20 I 1 BVerfSchG „von sich aus" die Informationen an die Strafverfolgungsbehörden. Die Vorschrift begründet damit eine Übermittlungspflicht, ohne dass es einer vorherigen Aufforderung bedarf.[608]

bb) Übermittlung nach § 19 I 1BVerfSchG

Als taugliche Übermittlungsregelung wird oftmals ergänzend auf die Vorschrift des § 19 I 1 BVerfSchG verwiesen. Diese Norm ermöglicht eine in das Ermessen der Dienste gestellte Übermittlung personenbezogener Daten an inländische öffentliche Stellen. Diese ist gestattet, wenn die Übermittlung zur Aufgabenerfüllung des Nachrichtendienstes erforderlich ist (Variante 1), der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung (Variante 2) oder sonst für Zwecke der öffentlichen Sicherheit (Variante 3) benötigt. Der Begriff der öffentlichen Stelle erfasst nach § 2 I 1, II BDSG unter anderem Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes und der Länder.[609] Die Staatsanwaltschaften sind Organe der Rechtspflege, sodass ein Rückgriff auf diese Übermittlungsvorschrift zu Strafverfolgungszwecken grundsätzlich denkbar ist.[610]

Die übrigen Voraussetzungen der einzelnen Übermittlungsvarianten sind sehr allgemein gefasst. Bei genauerer Betrachtung wird deutlich, dass diese nicht ohne Weiteres für eine Übermittlung zu repressiven Zwecken herangezogen werden können. In diesem Sinne ist die Verfolgung gewöhnlicher Kriminalität weder eine primäre Aufgabe der Dienste i.S.d. der Variante 1 noch erreicht sie das geforderte Schutzpotential i.S.d. Variante 2. Der Bereich der Staatsschutzdelikte kann zwar unter spezialpräventiven Gesichtspunkten zum Schutz der freiheitlichen demokratischen Grundordnung beitragen, dieser Deliktsbereich wird jedoch nach allgemeiner Ansicht abschließend von § 20 BVerfSchG erfasst. Ein Rückgriff auf die Varianten 1, 2 scheidet somit aus.[611] In Betracht kommt allerdings eine Subsumtion unter den Begriff der öffentlichen Sicherheit i.S.d. Variante 3. Dieses Merkmal entstammt dem Polizeirecht und erfasst nach allgemeiner Definition den Schutz des

---

608 So BT-Drs. 11/4306, S. 63; *Rehbein,* S. 118. Demgegenüber möchte *Zöller,* in: Roggan/Kutscha, S. 500, den Diensten einen gewissen Beurteilungs- und Ermessensspielraum zugestehen, der sich aber im Falle schwerer Straftaten zu einer Pflicht verdichten kann.

609 Seit der Änderung durch Gesetz vom 5.1.2007 (BGBl. I, 2007, S. 2, 4), mit Wirkung zum 11.1.2007, kann auf die Legaldefinition des § 2 BDSG zurückgegriffen werden.

610 So *Droste,* Handbuch, S. 519; *Gola/Schomerus,* BDSG, Erster Abschnitt, § 2 Rn. 11. Sonstige Anwendungsbereiche sind z.B. Einbürgerungsverfahren. Der nach § 11 StAG bestehende Einbürgerungsanspruch besteht nicht, wenn der Bewerber Bestrebungen i.S.d. BVerfSchG verfolgt, vgl. *Droste,* Handbuch, S. 521.

611 Zur grundsätzlichen subsidiären Anwendung dieser Variante vgl. *Wolff,* S. 125.

Staates und seiner Einrichtungen sowie die gesamte objektive Rechtsordnung und Individualrechtsgüter.[612] Das Strafgesetzbuch ist als Rechtsvorschrift ebenfalls Teil der geschützten Rechtsordnung, sodass ein Verstoß gegen eine Strafnorm zu einer Störung der öffentlichen Sicherheit führt.[613] Neben der präventiven Ausrichtung erfasst der Begriff der öffentlichen Sicherheit damit zugleich eine repressive Komponente.[614] Da die Strafverfolgungsbehörden nach § 152 II StPO zur Verfolgung von Straftaten verpflichtet sind, können sie strafrechtlich relevante Informationen zudem *für Zwecke* der öffentlichen Sicherheit benötigen.[615] Bei einer wortgetreuen Auslegung der Variante 3 von § 19 BVerfSchG könnten die Geheimdienste eine Übermittlung an die Strafverfolgungsbehörden damit parallel auf die Vorschrift des § 19 BVerfSchG stützen. Dies würde die Übermittlungsmöglichkeiten der Dienste auf Delikte außerhalb des Staatsschutzbereichs erweitern.

Die parallele Heranziehung von § 20 BVerfSchG im Bereich der Staatsschutzdelikte sowie von § 19 BVerfSchG im Bereich der sonstigen Kriminalität ist jedoch nicht unumstritten. Zum Verhältnis beider Übermittlungsvorschriften lassen sich im Wesentlichen drei unterschiedliche Auffassungen ausmachen.

Überwiegend wird von einer parallelen Anwendbarkeit des § 19 BVerfSchG ausgegangen.[616] Nach dieser Ansicht kommt der Vorschrift des § 20 BVerfSchG bereits aufgrund der unterschiedlichen Rechtsfolgen beider Normen kein abschließender Charakter zu. Während § 20 I BVerfSchG eine Übermittlungspflicht vorsieht, liegt die Entscheidung über eine Übermittlung nach § 19 I 1 BVerfSchG grundsätzlich im Ermessen der Dienste.[617] Die Übermittlungspflicht des § 20 BVerfSchG könne insofern die Ermessensvorschrift des § 19 BVerfSchG nicht ausschließen. Zudem seien die Anwendungsbereiche beider Vorschriften so unterschiedlich, dass ein Exklusivitätsverhältnis abgelehnt werden müsse. Die Vorschrift § 20 BVerfSchG beschränke sich von vorneherein auf Angelegenheiten des Staats- und Verfassungsschutzes. Eine ergänzende Übermittlung nach § 19 BVerfSchG für den Bereich der allgemeinen Kriminalität könne dadurch nicht ausgeschlossen werden.

---

612 So die wörtliche Fassung in BT-Drs. 11/4306, S. 63. Ebenso *Wolff,* S. 126; *Gusy,* Polizeirecht, S. 38.

613 Vgl. hierzu *Tettinger/Erbguth/Mann,* S. 190.

614 Vgl. *Gröpl,* S. 335.

615 Vgl. *Gröpl,* S. 336.

616 Die Argumente gegen eine abschließenden Regelung finden sich bei *Droste,* Handbuch, S. 518f, 543; *König,* S. 271f; *Pawlik,* JZ 2010, S. 696 Fn. 37; *Rehbein,* S. 115; *Rose-Stahl,* S. 105f; *Soiné,* NStZ 2007, S. 248. Ebenso *Lisken/Denninger,* in: Lisken/Denninger/Rachor, S. 117, der § 19 BVerfSchG als Globalermächtigung kritisiert.

617 Je nach Schwere des betroffenen Rechtsguts kann sich dieses Ermessen jedoch zu einer Übermittlungspflicht reduzieren. Nach *Droste,* Handbuch, S. 517, 543, handelt es sich bei dieser Entscheidung um eine Interessensabwägung.

Die Gegenansicht bejaht demgegenüber den abschließenden Charakter des § 20 BVerfSchG.[618] Nach dieser Ansicht würde eine ergänzende Heranziehung des § 19 BVerfSchG zu Strafverfolgungszwecken die Einhaltung des Trennungsgebotes in unzulässiger Weise in das Ermessen der Dienste stellen. Zudem sei die Vorschrift des § 19 BVerfSchG viel zu weit gefasst, um eine eingriffsintensive Übermittlung zu Strafverfolgungszwecken rechtfertigen zu können. Schließlich nehme der Titel des § 20 BVerfSchG im Gegensatz zu § 19 BVerfSchG ausdrücklich auf die Übermittlung zu repressiven Zwecken Bezug. Eine auf § 19 BVerfSchG gestützte Übermittlung zu Strafverfolgungszwecken würde daher der Gesetzessystematik widersprechen. Um eine rechtsstaatswidrige Umgehung des § 20 BVerfSchG zu verhindern, plädiert diese Ansicht im Anwendungsbereich der Nachrichtendienstgesetze daher für eine einschränkende Auslegung des Begriffs der öffentlichen Sicherheit.[619] Eine parallele, auf die Generalklausel des § 19 BVerfSchG gestützte Übermittlung an die Strafverfolgungsbehörden scheidet nach dieser Ansicht aus.

Eine dritte vermittelnde Ansicht bejaht die grundsätzliche Anwendbarkeit des § 19 BVerfSchG, sofern zugleich eine Übertragung der Wertungen des G10-Gesetzes erfolgt.[620] Die Vertreter stützen sich in Bezug auf die generelle Anwendbarkeit der Generalklausel auf die Argumente der ersten Ansicht. Die Schrankenübertragung wird mit dem Grundsatz der informationellen Gewaltenteilung, dem Zweckbindungsprinzip sowie den Bedürfnissen des Grundrechtsschutzes begründet.[621] Danach sei die Übermittlung nach § 19 BVerfSchG unter anderem auf die in den §§ 3 I, 3 Ia, 7 IV 1 G10 genannten Straftaten und damit auf Fälle schwerer Kriminalität zu begrenzen.

Bei einer Zugrundelegung der durch die Rechtsprechung entwickelten Grundsätze werden jedoch die Schwachstellen der einzelnen Ansätze deutlich.

Die uneingeschränkte Heranziehung von § 19 Var. 3 BVerfSchG durch die erste Ansicht lässt eine kritische Auseinandersetzung mit den Vorgaben der Zweckänderung vermissen. Obwohl es sich bei der Übermittlung von Geheimdienstinformationen um einen erheblichen Grundrechtseingriff handelt, wird die Regelung des

---

618 Vgl. etwa *Heine,* HRRS 2009, S. 541; *Schünemann,* NStZ 2008, S. 306f, stellvertretend zur Parallelnorm des § 9 I BNDG. Ebenso Löwe/Rosenberg-*Erb,* § 161 Rn. 82, der eine ausreichende Begründung aber schuldig bleibt und lediglich auf die rechtsstaatliche Notwendigkeit verweist. Im Ergebnis wohl auch *Salditt,* FS für Schaumburg, S. 1279.

619 Vgl. *Kelnhofer/Krug,* StV 2008, S. 665.

620 Vgl. hierzu *Sieber,* NJW 2008, S. 882. Eine solche Limitierung wurde bereits bei der im Jahre 1985 tagenden Konferenz der Datenschutzbeauftragten durch eine analoge Heranziehung der in § 7 III G10 a.F. genannten Katalogtaten diskutiert. Ebenfalls in diese Richtung Borgs-Maciejewski/Ebert-*Borgs*, § 3 BVerfSchG Rn. 37; *Riegel,* Computer und Recht 1986, S. 419. Generell für eine begrenzte Übermittlung *Roxin/Schünemann,* § 39 Rn. 24.

621 Vgl. *Sieber,* NJW 2008, S. 882.

§ 19 BVerfSchG als ausreichende Ermächtigung für eine Übermittlung erachtet ohne diese durch Übermittlungsschwellen zu begrenzen. Die Vorschrift des § 19 I 1 Var. 3 BVerfSchG erfüllt indes keine der an eine Zweckänderung gestellten Anforderungen. Dies lässt vermuten, dass der Gesetzgeber eine eingriffsintensive Zweckänderung zu repressiven Zwecken nicht in den Anwendungsbereich des § 19 BVerfSchG fallen lassen wollte. Darüber hinaus betrifft der Verweis auf die Gesetzessystematik und die unterschiedlichen Rechtsfolgen lediglich die Reichweite des § 20 BVerfSchG. Der Umkehrschluss, wonach § 19 BVerfSchG jegliche Formen der Übermittlung zulässt, kann daraus nicht gezogen werden.

Die von der vermittelnden Ansicht geforderte Begrenzung auf Fälle schwerer Kriminalität erfüllt die gerichtlichen Vorgaben zumindest teilweise. Allerdings fehlt eine Begründung, warum gerade der Katalog des G10 herangezogen werden soll. Zudem ist unklar, ob sich die G10-Wertungen nur auf die Straftatkataloge oder zugleich auf die dort vorzufindenden Übermittlungsschwellen beziehen. Allerdings sprechen für die Übertragbarkeit der G10-Wertungen gute Gründe. Zum einen verweist die Aufgabennorm des § 1 G10 selbst auf die allgemeinen Aufgaben nach den Nachrichtendienstgesetzen und stellt damit bereits einen natürlichen Konnex zwischen den Gesetzen her. Zum anderen ist die Heranziehung der G10-Wertungen auch unter chronologischen Gesichtspunkten nicht zu beanstanden. Nach seinem erstmaligen Inkrafttreten im Jahre 1968 ohne Übermittlungsvorschriften wurde das G10 in seiner letzten Neufassung 2001 um die heutigen Übermittlungsvorschriften in den §§ 4, 7 G10 ergänzt.[622] Die Wertungen der jüngeren G10-Normen können damit theoretisch zur Ergänzung des älteren BVerfSchG herangezogen werden, da dieses erstmals 1950 und zuletzt 1990 neu gefasst wurde.[623] Eine Übertragung der G10-Kataloge macht unter praktischen Gesichtspunkten allerdings nur Sinn, wenn diese Straftaten nicht bereits vom Katalog des § 20 BVerfSchG abgedeckt werden. Eine parallel zur Übermittlungspflicht bestehende Ermessensnorm mit einem faktisch identischen Straftatkatalog würde zu Widersprüchen innerhalb des BVerfSchG führen. Stellt man die verschiedenen Übermittlungskataloge jedoch konkret gegenüber, ist diese Deckungsgleichheit gegeben. Insofern werden fast sämtliche Delikte der §§ 4, 7 G10 über die verschiedenen Verweisungsketten auch von § 20 I BVerfSchG erfasst.[624] Der Gesetzgeber hätte eine solche Parallelität durch eine ausdrückliche Schrankenübertragung bei der Reformierung in Jahr 2007[625] mittels einer entsprechenden Ergänzung des § 19 I BVerfSchG

---

[622] Zur ursprünglichen Fassung aus dem Jahr 1968 siehe BGBl. I, 1968, S. 949. Zur Neufassung 2001 siehe BGBl. I, 2001, S. 1254, berichtigt S. 2298.

[623] Zur Fassung von 1950 siehe BGBl. I, 1950, S. 682, zur Fassung von 1990 siehe BGBl. I, 1990, S. 2954, 2975f.

[624] Nicht von der Verweisung des § 20 BVerfSchG erfasst sind lediglich die folgenden Delikte: § 146; §§ 151–152a; §§ 249–251; 255; 305a; 316a StGB.

[625] Mit dem Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes vom 5.1.2007 (BGBl. I, 2007, S. 2) wurden u.a. Teile des BVerfSchG reformiert.

herstellen können. Dort wurden bereits andere Absätze des § 19 BVerfSchG zur Klarstellung neu gefasst.[626] Zu einer solchen Konkretisierung ist es hinsichtlich der Übermittlungsbefugnis nach § 19 I BVerfSchG indes nicht gekommen. Es bleibt allerdings unklar, ob der Gesetzgeber auf eine entsprechende Anpassung bewusst verzichtet hat.

Die dritte Ansicht ist ebenfalls kritisch zu sehen. Obwohl die einzelnen Argumentationsansätze zum Teil begründete Zweifel am abschließenden Charakter des § 20 BVerfSchG wecken, setzt sie sich nicht mit den bedenkenswerten Begründungsansätzen der Gegenansichten auseinander. Diese hätten insofern jedoch zumindest einer Erwiderung bedurft.

Da die Übermittelbarkeit von Geheimdienstinformationen zu Strafverfolgungszwecken eine erhebliche praktische Relevanz aufweist, wird für diese Problematik ein eigener Begründungs- beziehungsweise Lösungsansatz herausgearbeitet. Die Beurteilung der Übermittlungsvorschriften orientiert sich primär an den klassischen Auslegungsmethoden, den Vorgaben der Zweckbindung und des Trennungsgebots. Sowohl der Wortlaut als auch die systematische Einordnung des § 19 BVerfSchG stehen einer Übermittlungsbefugnis zu Zwecken der Strafverfolgung grundsätzlich offen gegenüber. Zweifel an einer uneingeschränkten Übermittlungsbefugnis ergeben sich jedoch unter Berücksichtigung der Gesetzesmaterialien. Der heutige § 19 BVerfSchG fand sich in dem Gesetzesentwurf der Bundesregierung aus dem Jahr 1989 im weitgehend identisch formulierten § 14 I a.F. BVerfSchG. Der Gegenpart des heutigen § 20 I BVerfSchG war in § 15 a.F. BVerfSchG normiert und gestattete bereits damals die Übermittlung an die Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes.[627] In einem Entschließungsantrag kritisierte die Fraktion der Grünen die auf Staatsschutzdelikte begrenzte Übermittlungsvorschrift des § 15 BVerfSchG a.F. als viel zu pauschal.[628] Diese war laut der Gesetzesbegründung als Spezialvorschrift zu § 14 I a.F. BVerfSchG konzipiert.[629] Auf die Heranziehung der Generalklausel des § 14 I a.F. BVerfSchG zu allgemeinen repressiven Zwecken wurde dagegen überhaupt nicht eingegangen, obwohl diese bei unterstellter Anwendbarkeit sogar noch umfassendere Übermittlungen zugelassen hätte. Die Grünen, die zu diesem Zeitpunkt sogar die Abschaffung des Verfassungsschutzes forderten,[630] hätten eine der-

---

626 Vgl. etwa zu § 19 IV BVerfSchG in BT-Drs. 16/2921, S. 17.

627 Vgl. BT-Drs. 11/4306, S. 28.

628 Vgl. BT-Drs. 11/7277, S. 2.

629 Vgl. BT-Drs. 11/4306, S. 63. Ebenso BT-Drs. 618/88, S. 167. Nach der Gesetzesbegründung war eine Übermittlung in Angelegenheiten des Staats- und Verfassungsschutzes auf der Grundlage des § 14 I a.F. BVerfSchG ausdrücklich ausgeschlossen.

630 Vgl. u.a. den Verweis auf die Notwendigkeit einer Auflösung der Nachrichtendienste BT-Drs. 11/7277, S. 1. Zur aktuellen Diskussion nach dem NSU-Skandal vgl. *Gusy,* ZRP 2012, S. 230f.

art weite Übermittlungsbefugnis wohl kaum diskussionslos akzeptiert. Die Tatsache, dass die Heranziehung des § 14 a.F. BVerfSchG zu Strafverfolgungszwecken überhaupt nicht diskutiert wurde, lässt vermuten, dass die am Gesetzgebungsverfahren Beteiligten von vorneherein nicht von einer Einbeziehung repressiver Zwecke in die Generalklausel ausgingen.[631] Die wörtliche Übernahme dieser Vorschrift in den jetzigen § 19 BVerfSchG spricht dafür, dass der spätere Gesetzgeber den Willen des damaligen Gesetzgebers übernommen hat.

Dieses Ergebnis wird durch teleologische Gesichtspunkte gestützt. Wie bereits die zweite und dritte Ansicht zu Recht fordern, ist die Übermittlung von Informationen durch die Dienste an die Strafverfolgungsbehörden zu begrenzen. Würde man den Diensten abseits ihres besonderen und umfassenden Beobachtungsauftrags eine umfassende Übermittlung gestatten, könnten sich die Dienste entgegen den Vorgaben des Trennungsgebots faktisch einen Vollzugsarm schaffen. Durch die Bindung an das Legalitätsprinzip wären die Strafverfolgungsbehörden zumeist zu weiteren Ermittlungen verpflichtet. Aufgrund der Ausgestaltung als Ermessensvorschrift könnten damit letztlich die Dienste und nicht die Strafverfolgungsbehörden auf der Grundlage des § 19 BVerfSchG über die Einleitung eines Ermittlungsverfahrens entscheiden. Dies würde dem Zweck des Legalitätsprinzips zuwiderlaufen.

Letztlich ist der Wortlaut der Vorschrift des § 19 BVerfSchG zu weit geraten, um eine verfassungskonforme Übermittlung zu Strafverfolgungszwecken rechtfertigen zu können. Um die Verfassungsmäßigkeit der Norm zu wahren, ist der Begriff der öffentlichen Sicherheit vorliegend im Wege einer teleologischen Reduktion auf seinen präventiven Bedeutungsgehalt zu reduzieren. Der Begriff der Sicherheit ist im Anwendungsbereich der Nachrichtendienstgesetze somit ausschließlich als präventive Sicherheit zu verstehen. Eine Übermittlung zu Zwecken der Gefahrenabwehr bleibt damit weiterhin möglich, während eine Übermittlung zur Verfolgung einfacher Straftaten ausscheidet. Der Einwand, dass sich der Staat durch eine derartige Begrenzung künstlich vorhandenen Wissens beraubt, überzeugt nicht. Die Idee einer einheitlichen Staatsgewalt mit einem staatlichen Allgemeinwissen, welches dem Staat und sämtlichen staatlichen Einrichtungen zusteht, ist spätestens seit der gesetzlichen Normierung des Datenschutzrechts überholt. Das Erfordernis einer informationellen Gewaltenteilung zwischen den verschiedenen staatlichen Institutionen ist im Zusammenhang mit personenbezogenen Daten unbestritten.[632] Eine Spontanübermittlung im Anwendungsbereich der Nachrichtendienstgesetze kann damit nicht auf § 19 I BVerfSchG, sondern ausschließlich auf die in § 20 I 1 BVerfSchG genannten Voraussetzungen gestützt werden.

---

631 Bloß andeutend insofern BT-Drs. 11/4306, S. 86 rechte Spalte.

632 Vgl. *Kretschmer,* JURA 2006, S. 439, und den 1. Tätigkeitsbereich des Bundesbeauftragten für den Datenschutz in BT-Drs. 8/2460, S. 24.

cc) Sonstige Übermittlungsregeln, insbesondere G10

Für die Übermittlung von G10-Daten wurden mit § 4 IV Nr. 2, V, VI G10 für die Individualüberwachung und § 7 IV 2, V, VI G10 für die strategische Aufklärung eigenständige Übermittlungsvorschriften geschaffen. Die das G10 durchziehende Zweiteilung der Erhebungsmaßnahmen setzt sich damit in der Regelungstechnik der Übermittlungsvorschriften fort.[633]

Die umfassende Verweisungspraxis führt allerdings zu einem gewissen Gleichlauf der verschiedenen Übermittlungsregeln. Gemeinsame Merkmale der §§ 4, 7 G10 finden sich sowohl auf formeller wie auf materieller Ebene. In formeller Hinsicht werden die Übermittlungsentscheidungen einheitlich durch einen Bediensteten der Dienste mit der Befähigung zum Richteramt getroffen.[634] Darüber hinaus finden sich parallele Protokollierungs-,[635] Überprüfung-, Kennzeichnungs- und Lösungspflichten[636] sowie die Bindung des Empfängers an den Übermittlungszweck.[637] In materieller Hinsicht ist jeweils die Erforderlichkeit der Übermittlung zur Aufgabenerfüllung des Empfängers nachzuweisen.[638] Zudem knüpfen beide Übermittlungsregime mit dem Erfordernis „bestimmter Tatsachen" an identische Verdachts- beziehungsweise Übermittlungsschwellen an.[639] Diese im Vergleich zum vorherigen Rechtszustand angehobene Übermittlungsschwelle ist eine Reaktion des Gesetzgebers auf das Urteil des Bundesverfassungsgerichts vom 14.7.1999.[640] Im damaligen Urteil lehnten die Richter bei einer Übermittlung zu Strafverfolgungszwecken eine Absenkung unter die nach § 100a StPO für die Strafverfolgungsbehörden geltende Eingriffsschwelle ab.[641] Die Rechtsgutsverletzung sei bereits erfolgt, sodass es nicht mehr um die Verhinderung, sondern ausschließlich um die Sanktionierung der Tat ginge. Bei einer Übermittlung der Dienste zu Strafverfolgungszwecken sei damit eine Angleichung an die Verdachtsschwelle verfassungsrechtlich geboten. In der Folge erhöhte der Gesetzgeber die

---

633 Vgl. zur Übermittlung von G10-Daten *König,* S. 273ff.

634 Vgl. § 4 V 3 sowie § 7 V 3 G10.

635 Vgl. die §§ 4 V 3, 7 V 2 G10.

636 Vgl. die §§ 4 VI 2, 7 VI 2 G10 sowie § 6 G10 gegebenenfalls i.V.m. § 7 VI 3 G10.

637 Vgl. die §§ 4 VI 1, 7 VI 1 G10.

638 Vgl. § 4 VI 2 sowie § 7 V 1 G10.

639 Vgl. BT-Drs. 14/5655, S. 16 und S. 21.

640 BVerfGE 100, 313ff. Weitere Folgen des Urteils waren die Einführung bzw. Neuformulierung von Kennzeichnungs-, Protokollierungs-, Überprüfungs- und Löschungspflichten sowie eine strenge Zweckbindung, vgl. BT-Drs. 14/5655, S. 13.

641 So BVerfG NJW 2000, S. 55, 66. Das Bundesverfassungsgericht hat es dabei allerdings dem Gesetzgeber überlassen, ob er den Straftatkatalog auf wenige Delikte mit vergleichsweise niedriger Übermittlungsschwelle beschränkt oder einen erweiterten Katalog an eine höhere Übermittlungsschwelle knüpft. Der Gesetzgeber hat sich letztlich für eine erhöhte Übermittlungsschwelle entschieden, vgl. BT-Drs. 14/5655, S. 21.

Verdachtsbasis auf das Vorliegen bestimmter Tatsachen für den Verdacht einer Katalogtat und übernahm damit die vom BVerfSchG geforderte Tatsachenbasis.[642]

Unterschiede zwischen den Übermittlungsregeln der §§ 4, 7 G10 ergeben sich allerdings in Bezug auf die zur Übermittlung berechtigenden Katalogtaten. Der exakte Umfang der Straftatkataloge ist aufgrund einer sehr komplexen Verweisungsstruktur kaum feststellbar.

Für die strategische Überwachung verweist § 7 IV 2 G10 auf den abschließenden Katalog des § 7 IV 1 G10. § 7 IV 1 Nr. 1 G10 listet Straftaten wie die Bildung einer terroristischen Vereinigung, Geld- und Wertzeichenfälschungen, Geldwäsche, Betäubungsmitteldelikte sowie Delikte nach dem Außenwirtschaftsgesetz und dem Kriegswaffenkontrollgesetz auf. Die Vorschrift des § 7 IV 1 Nr. 2a G10 ergänzt diesen Katalog durch eine Verweisung auf Straftaten nach § 3 I 1 Nr. 1 bis Nr. 5 und Nr. 7 G10 und erweitert ihn damit unter anderem auf Staatsschutzdelikte i.e.S., wie etwa Delikte des Friedens- und Hochverrats sowie der Gefährdung des demokratischen Rechtsstaats und der äußeren Sicherheit.[643] Daneben werden schwere Straftaten des 16., 18., 20. und 28. Abschnitts des StGB mit einbezogen, die unter anderem Mord, Totschlag, Menschenhandel, Menschenraub, Raub- und Erpressungsdelikte sowie gemeingefährliche Straftaten beinhalten. Die mangels Verweisung auf § 3 I 1 Nr. 6 vermeintlich ausgenommenen Delikte werden ihrerseits durch die ebenfalls in § 7 IV 1 Nr. 2a G10 erfolgende Verweisung auf den Katalog des § 129a StGB erfasst.

Für die Individualüberwachung verweist § 4 IV Nr. 2 G10 auf die Kataloge des § 3 I, Ia und § 7 IV 1 G10. Durch die Einbeziehung des § 7 IV 1 G10 werden die zur Übermittlung berechtigenden Katalogtaten für die strategische und Individualüberwachung weitgehend angeglichen. Da sowohl die Delikte des § 3 I G10 als auch des § 7 IV 1 G10 direkt oder vermittelt über § 129a StGB Anwendung finden, sind die Übermittlungskataloge der strategischen Überwachung und der Individualüberwachung weitgehend identisch. Selbst der Verweis auf § 3 Ia G10 i.V.m. § 23a I, II ZFdG erstreckt sich auf ähnliche Straftaten nach dem Kriegswaffenkontrollgesetz.

Im Ergebnis unterliegt die Übermittlung von G10-Daten weitgehend einheitlichen Rahmenbedingungen.[644] Die komplexe Verweisungsstruktur mit zahlreichen

---

[642] Vgl. BT-Drs. 14/5655, S. 21. Diese Lösung wird kritisiert, da eine solche Verdachtslage nur geringe Anforderungen stellt, vgl. *Frister,* FS für Bemmann, S. 543; *Roggan,* in: Roggan/Kutscha, S. 429. Es ist sogar von einer Alibifunktion der normierten Verdachtslage die Rede, vgl. *Frister,* StV 1996, S. 455. Zweifelnd in Bezug auf die tatsächliche Verschiedenheit der Verdachtsschwellen *Gröpl,* NJW 1996, S. 102.

[643] Folglich werden fast sämtliche Delikte des ersten und zweiten Abschnitts des Besonderen Teils des StGB erfasst, vgl. *König,* S. 276.

[644] Zu den unterschiedlichen Schwellen für eine Übermittlung zu präventiven Zwecken vgl. *König,* S. 276ff.

Doppel- und Unterverweisen erschwert indes die Herausarbeitung eines klaren Übermittlungskatalogs.[645] Dessen ungeachtet wird eine Schwerpunktsetzung auf Straftaten im Bereich des Staatsschutzes, des internationalen Terrorismus sowie der schweren Straftaten gegen die Person deutlich. Die Übermittlung von G10-Daten ist damit primär auf schwerwiegende beziehungsweise sicherheitsrelevante Delikte beschränkt, bei denen von einem gesteigerten Strafverfolgungsinteresse ausgegangen werden kann.[646] Aufgrund dieser Begrenzungen fällt die Anzahl der an die Strafverfolgungsbehörden übermittelten G10-Daten relativ gering aus. Obwohl die Anzahl der nachrichtendienstlich als relevant eingestuften Meldungen drei- bis vierstellige Zahlen erreicht, bewegt sich die Zahl der an die Strafverfolgungsbehörden weitergeleiteten Meldungen im geringen zwei- oder sogar einstelligen Bereich.[647]

dd) Zwischenergebnis

Die Übermittlung nachrichtendienstlicher Erkenntnisse zu Zwecken der Strafverfolgung unterliegt im Anwendungsbereich der Nachrichtendienstgesetze den Voraussetzungen des § 20 I 1 BVerfSchG, die entweder direkt oder vermittelt über die Verweisungsnormen zur Anwendung kommen. Die Weitergabe von Geheimdienstinformationen zu Strafverfolgungszwecken ist damit nur bei speziellen Staatsschutzdelikten gestattet, für die zusätzlich eine dem Strafverfolgungssektor vergleichbare Tatsachenbasis vorliegen muss. Diese Erkenntnis konnte für die Übermittlung von Telekommunikationsdaten bestätigt werden, die nach den §§ 4, 7 G10 „bestimmte Tatsachen" für abschließend benannte schwerwiegende Katalogtaten fordern. Die Übermittlungsregeln begrenzen den Erkenntnisaustausch damit auf besonders schwerwiegende Delikte oder solche von sicherheitspolitischer Relevanz.

b) Übermittlung auf Anfrage

Außer durch Spontanübermittlung durch die Geheimdienste kann die Übermittlung von Geheimdienstinformationen auf ein Ersuchen der Strafverfolgungsbehörden hin erfolgen. Der Abruf der Daten begründet ebenfalls einen Grundrechtsein-

---

[645] Dennoch hat der EGMR die Übermittlung von Daten aus Abhörmaßnahmen nach dem G10-Gesetz als mit Art. 8 II EMRK vereinbar erklärt, vgl. EGMR NJW 2007, S. 1433, 5. Leitsatz.

[646] So *Grawe,* S. 126.

[647] Im Berichtszeitraum 1.7.2002 bis 30.6.2003 wurden von 534 Meldungen nur 18 Meldungen an die Strafverfolgungsbehörden weitergeleitet. Diese bezogen sich allesamt auf Delikte nach § 129a StGB; vgl. BT-Drs. 15/2616. Im Zeitraum 1.5.1996 bis 31.12.1997 wurden von 2069 Meldungen sogar nur 2 Meldungen weitergeleitet, vgl. BT-Drs. 13/9938, S. 2. Ebenfalls unter Verweis auf die geringe Effizienz *Kühne,* Strafprozessrecht, Rn. 389.

griff und bedarf daher einer eigenständigen Rechtsgrundlage.[648] Die Grundlage eines solchen Ersuchens bildet § 161 I 1 StPO. Dieser ermächtigt die Staatsanwaltschaft im Rahmen eines laufenden Ermittlungsverfahrens von allen Behörden Auskunft zu verlangen.[649] Sobald die Verfahrensherrschaft auf das Gericht übergeht, steht dieses Auskunftsrecht den Gerichten zu.[650]

Die von § 161 I 1 StPO aufgestellten formellen und materiellen Voraussetzungen sind sehr gering. Erforderlich sind lediglich ein formelles Auskunftsersuchen vonseiten der Staatsanwaltschaft, ein tauglicher Adressat sowie das Bestehen eines Anfangsverdachts. Bei einer Anfrage an die Dienste während eines Ermittlungsverfahrens sind diese Voraussetzungen unproblematisch erfüllt. Die grundsätzliche Zulässigkeit eines Ersuchens an die Nachrichtendienste wird in § 17 I BVerfSchG anerkannt.[651] Diese Vorschrift beschränkt die Anfrage von vorneherein auf die bei den Diensten bereits vorhandenen beziehungsweise aus allgemein zugänglichen Quellen gewonnenen Informationen.[652] Dies verhindert, dass die ersuchende Behörde unter dem Vorwand eines Ersuchens den Diensten einen Ermittlungsauftrag erteilt. Darüber hinaus wird hierdurch zusammen mit dem Amtshilfeverbot des § 8 III BVerfSchG einer dem Trennungsgebot zuwiderlaufenden Vereinigung polizeilicher und geheimdienstlicher Befugnisse vorgebeugt.[653]

Bei einer unreflektierten Anwendung des § 161 I StPO wären die Dienste bei einer Anfrage damit in den meisten Fällen zur Erteilung der erbetenen Auskunft verpflichtet.[654] Die damit verbundene Informationsweitergabe wäre jedoch anders als die Eigeninitiativübermittlung nicht an bestimmte Übermittlungskataloge, sondern lediglich an das Vorliegen eines Anfangsverdachts gebunden. Diese abweichenden Übermittlungsstandards werfen erneut die Frage nach dem Verhältnis unterschiedlicher Übermittlungsregime auf. Vorliegend ist zu klären, ob bei einer Anfrage nach § 161 I StPO zusätzlich die Vorgaben der Nachrichtendienstgesetze nach §§ 20ff BVerfSchG als Spezialregelungen zu beachten sind.[655] Hierzu werden schwerpunktmäßig zwei Modelle vertreten (siehe Abb. 2, S. 106).

---

[648] BVerfG, 1 BvR 1299/05 vom 24.1.2012, 2. Leitsatz.

[649] Vgl. Löwe/Rosenberg-*Erb,* § 161 Rn. 4; *König,* S. 284.

[650] Dies gilt sowohl für das eröffnende als auch erkennende Gericht; vgl. BGH NJW 1981, S. 1052; Löwe/Rosenberg-*Erb,* § 161 Rn. 8; *Rieß,* FS für Hilger, S. 175.

[651] So *Rehbein,* S. 122.

[652] So bereits BT-Drs. 11/7235, S. 108; *König,* S. 265; *Zöller,* Informationssysteme, S. 324.

[653] Vgl. *Droste,* Handbuch, S. 478; *König,* S. 265.

[654] Zur Auskunftspflicht vgl. LG Frankfurt NJW 1980, S. 1478f; *Meyer-Goßner*, § 161 Rn. 1a.

[655] Die Beantwortung dieses Streitstands hängt eng mit der Diskussion bezüglich der Gesetzgebungskompetenz bei Übermittlungsregeln zusammen. Zu den unterschiedlichen Modellen vgl. *Bertram,* S. 308ff; *König,* S. 289; *Paeffgen,* FS für Hilger, S. 155f; *Zöller,* in: Roggan/Kutscha, S. 461.

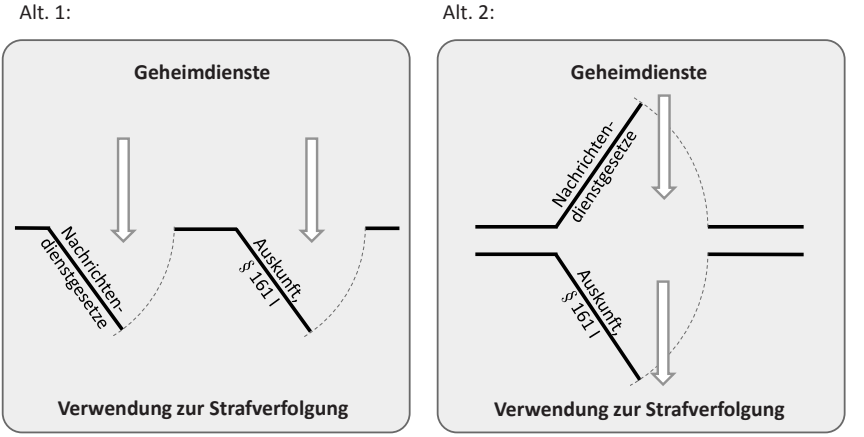

Abbildung 2: Nach Alt.1 gestattet § 161 I StPO die Übermittlung von Geheimdienstinformationen unabhängig von den Nachrichtendienstgesetzen; nach dem sog. Doppeltürenmodell (Alt. 2) müssen sowohl § 161 I StPO als auch die Nachrichtendienstgesetze die Übermittlung gestatten

Nach dem ersten Modell handelt es sich bei § 161 StPO um eine eigenständige Übermittlungsvorschrift, die eine Übermittlung unabhängig von den Vorgaben der Nachrichtendienstgesetze gestattet.[656] Eine Übermittlung nach § 161 I StPO wäre danach nur an das Vorliegen eines Anfangsverdachts gebunden.[657]

Das erste Modell wird im Wesentlichen auf vier Erwägungen gestützt. Als erstes Argument wird die allgemeine Amtshilfepflicht des Art. 35 I GG angeführt. Danach sei die ersuchte Behörde bei einer Anfrage nach § 161 I StPO zur Übermittlung verpflichtet. Die Vorgaben der Nachrichtendienstgesetze müssten beim Greifen der Amtshilfepflicht nicht beachtet werden. Zweitens gälten die nachrichtendienstlichen Übermittlungsschranken allein bei Eigeninitiativübermittlungen und könnten daher nicht auf eine Anfrageübermittlung übertragen werden. Als drittes Argument werden Anhaltspunkte bezüglich der Entstehungsgeschichte der Übermittlungsnormen angeführt. Nach der damaligen Regierungsvorlage sollten die Auskunftsrechte der Staatsanwaltschaften weiterhin uneingeschränkt bestehen bleiben.[658] Es sei insofern verfassungsrechtlich geboten, „Straftaten aller Art effektiv zu verfolgen […] und dabei auf Informationen des Bundesamtes für Verfassungs-

---

656 So *Rehbein,* S. 119; *Soiné,* NStZ 2007, S. 249.

657 In Zuständigkeitsfragen entspricht dies der Ansicht, welche die Kompetenz zum Erlass von Übermittlungsvorschriften allein dem Gesetzgeber der Empfangsbehörde zuweist.

658 Vgl. BT-Drs. 11/4306, S. 86f.

schutz zurückzugreifen".[659] Viertens wird die Eigenständigkeit des § 161 I StPO mit einem Umkehrschluss zu § 96 StPO begründet. Diese Vorschrift gestattet einer Behörde die Zurückhaltung von Schriftstücken oder Akten, wenn die oberste Dienstbehörde in einer rechtmäßigen Sperrerklärung drohende Nachteile für das Wohl des Bundes oder eines Landes feststellt. Ein derartiges Verweigerungsrecht wäre überflüssig, wenn die Dienste ohnehin eine Übermittlung unter Verweis auf die Vorgaben der Nachrichtendienstgesetze verweigern könnten.

Diese für eine unbegrenzte Anfrageübermittlung angeführten Argumente sind jedoch kritisch zu sehen. Das erste Argument verkennt den Regelungsumfang des Art. 35 I GG. Dieser kann eine ersuchte Behörde lediglich in dem für sie geltenden Rechts- und Kompetenzrahmen verpflichten.[660] Da die Nachrichtendienstgesetze eine Übermittlung nur bei Vorliegen bestimmter Übermittlungsschwellen und Delikte gestatten, müssen diese Grenzen bei der Gewährung von Amtshilfe ebenfalls beachtet werden. Diese Übermittlungsbefugnisse können insofern nicht auf der Grundlage des Art. 35 I GG erweitert werden.[661] Das zweite Argument, wonach sich die Übermittlungsschranken von vorneherein auf die Eigeninitiativübermittlung begrenzen, wird von dieser Ansicht zum Teil selbst nicht stringent verfolgt. Dies wird nicht zuletzt daran deutlich, dass manche Vertreter der Gegenansicht ihrerseits von der Anwendbarkeit der Übermittlungssperre des § 23 BVerfSchG auf eine Anfrageübermittlung ausgehen.[662] Eine Begründung, warum bei der Übermittlungssperre nicht aber bei der Übermittlungsvorschrift der spezialgesetzliche Charakter der Nachrichtendienstgesetze anerkannt wird, fehlt. Der im Rahmen des dritten Arguments angeführte Verweis auf die Entwicklungsgeschichte überzeugt ebenfalls nicht. Der Vermerk im Gesetzesentwurf stellt lediglich klar, dass die Staatsanwaltschaft entsprechende Informationen verlangen darf. Eine Aussage, ob die Nachrichtendienste letztlich zu einer Übermittlung befugt sind, wird dadurch nicht getroffen. Da es sich um die Kompetenzbereiche unterschiedlicher Behörden handelt, werden durch die nachrichtendienstlichen Übermittlungsschwellen die Befugnisse der Staatsanwaltschaft gerade nicht beschnitten. Entgegen dem vierten Argument ist das Verweigerungsrecht des § 96 StPO schließlich nicht von vorneherein überflüssig, da auch die Vorschrift des § 20 BVerfSchG im Grundsatz eine Übermittlungspflicht begründet. Zudem kann die vorrangige Anwendbarkeit der Strafprozessordnung nicht unter Rückgriff auf eine andere Norm der Strafprozessordnung begründet werden.

---

659 Vgl. BT-Drs. 11/4306, S. 87.

660 So Maunz/Dürig-*Maunz,* Art. 35 Rn. 1.

661 So etwa Maunz/Dürig-*Maunz,* Art. 35 Rn. 1; *Schneider,* NJW 1978, S. 1602.

662 So etwa *Rehbein,* S. 121.

Nach einem zweiten Modell sind die Nachrichtendienstgesetze als Spezialvorschrift bei jeder Übermittlung zu beachten.[663] Dementsprechend müssten bei einer Anfrage stets ergänzend die Voraussetzungen der Nachrichtendienste und damit unter anderem der Verdacht auf eine der dort genannten Katalogtaten gegeben sein.[664] Diese Ansicht ist aus kompetenzrechtlichen, verfassungsrechtlichen und systematischen Gründen vorzugswürdig.

Für die Beachtung nachrichtendienstlicher Vorgaben können *kompetenzrechtliche* Erwägungen herangezogen werden. Bei einer Übermittlung handelt es sich um eine Zweckentfremdung, die im Ausgangspunkt nur durch den Primärgesetzgeber gestattet werden kann. Die mit der Informationserhebung verbundene Eingriffstiefe kann nicht einseitig durch die Zweckerweiterung einer dritten Behörde vertieft werden.[665] Die Verantwortung für den mit der Übermittlung verbundenen Eingriff und damit das erstmalige Entlassen der Information aus dem nachrichtendienstlichen Bereich trägt insofern der Primärgesetzgeber.[666] In Bezug auf Geheimdienstinformationen müssen damit stets die Öffnungsklauseln der Nachrichtendienstgesetze beziehungsweise des G10-Gesetzes überwunden werden. Bildlich gesprochen handelt es sich bei diesen Öffnungsklauseln um eine Art Nadelöhr. Erst wenn die nachrichtendienstlichen Erkenntnisse diese schmale Öffnung passiert haben, können sie einer weiteren Verwendung zugänglich gemacht werden. Die Norm des § 161 I StPO verdeutlicht lediglich die Zulässigkeit eines staatsanwaltschaftlichen Ersuchens, ohne die an die Übermittlung zu stellenden Anforderungen abschließend zu regeln.[667] Die nachrichtendienstlichen Vorgaben müssen daher aus kompetenzrechtlichen Gründen stets vorrangig beachtet werden. Dieser Aspekt ist insbesondere in Bezug auf die landesgesetzlichen Nachrichtendienstgesetze von Bedeutung.

Daneben kann die Begrenzung auf verfassungsrechtliche Erwägungen gestützt werden. Würde § 161 I StPO als einzige Übermittlungsgrundlage herangezogen werden, könnte die Staatsanwaltschaft eine Informationsübermittlung ungeachtet

---

[663] So etwa *König,* S. 259, 285; SK-StPO-*Wohlers,* § 161 Rn. 31. Ebenso Löwe/Rosenberg-*Erb,* § 161 Rn. 82. Die Bezugnahme auf die Verwertbarkeit ist unschädlich, da die Verwertbarkeit von Geheimdienstdaten zu Strafverfolgungszwecken zunächst die Übermittelbarkeit zu Strafverfolgungszwecken voraussetzt. Ähnlich *Baumann,* FS für Posser, S. 307; *Diemer,* NStZ 2005, S. 668. Von einer Vorrangstellung der Nachrichtendienstgesetze ausgehend *Gröpl,* S. 317.

[664] In Zuständigkeitsfragen entspricht dies wohl dem vorliegend favorisierten Modell der doppelten Tür, welches die Gesetzgebungskompetenz zwischen dem Gesetzgeber der Primär- und Sekundärnutzung aufteilt. Das Doppeltürenmodell wurde im Beschluss des BVerfG vom 24.2.2012, 1 BvR 1299/05 bestätigt. Ebenso *Singelnstein,* ZStW 120 (2008), S. 863.

[665] So *Singelnstein,* ZStW 120 (2008), S. 863.

[666] Zur Verantwortung der übermittelnden Stelle hinsichtlich der Zulässigkeit der Übermittlung vgl. *Droste,* Handbuch, S. 475 Fn. 1532; *König,* S. 259.

[667] In diesem Sinne *König,* S. 285.

der Schwere des maßgeblichen Delikts verlangen.[668] Bei einer Übermittlung der Dienste an die StrafverfolgungsSbehörden handelt es sich jedoch um eine gravierende Zweckentfremdung, die den Anforderungen der Zweckänderung genügen muss. Die Vorschrift des § 161 I StPO erfüllt indes keine der materiellen Anforderungen der Rechtsprechung. Selbst in Bezug auf die geforderte Normenklarheit würde der Bürger die Übermittlungsvorschriften stets in dem Gesetz vermuten, in dem bereits Aufgaben und Befugnisse der übermittelnden Behörden geregelt werden.[669]

Dieses Argument wird durch systematische Erwägungen gestützt. Der Gesetzgeber geht zum Teil selbst von einem Vorrangverhältnis der Nachrichtendienstgesetze aus; etwa im Bereich der personenbezogenen Daten. Nach §§ 15 I i.V.m. § 14 II Nr. 7 BDSG unterliegt die Übermittlung von personenbezogenen Daten zu Zwecken der Strafverfolgung grundsätzlich den Vorgaben des Bundesdatenschutzgesetzes (BDSG).[670] Im Anwendungsbereich der Nachrichtendienstgesetze werden diese Regelungen durch § 27 BVerfSchG allerdings ausdrücklich ausgeschlossen, da die umfassenden Übermittlungspflichten des BDSG nach Ansicht des Gesetzgebers nicht mit den nachrichtendienstlichen Geheimhaltungsinteressen vereinbar sind.[671] Die differenzierten datenschutzrechtlichen Schutzvorkehrungen werden insofern durch die noch spezielleren Regelungen der Nachrichtendienstgesetze überlagert. Da die Regeln des BDSG grundsätzlich bei einer Anfrageübermittlung nach § 161 I StPO zur Anwendung kommen, muss die gesetzlich angeordnete Vorrangstellung der Nachrichtendienstgesetze erst Recht im Verhältnis zur Generalklausel des § 161 I StPO beachtet werden.[672]

Vor allem kann für eine Beachtung der nachrichtendienstlichen Übermittlungsvorschriften der Beschluss des Bundesverfassungsverfassungsgerichts vom 24.1.2012 angeführt werden.[673] In diesem Urteil wurde ausdrücklich das „Doppeltürenmodell“ zugrunde gelegt. In seinem Beschluss unterscheidet das Bundesverfassungsgericht bei einer Datenübermittlung zwischen der Datenübermittlung seitens der auskunftserteilenden Stelle und dem Datenabruf seitens der auskunftssuchenden Stelle. Dieser Vorgang bedarf nach Ansicht des Gerichts zweier korrespondierender Rechtsgrundlagen, die bildlich wie eine „eine Doppeltür zusammenwirken müssen“. Der Informationsaustausch müsse demnach von zwei Seiten gestattet werden.[674] Das Gericht gibt weiterhin zu erkennen, dass diese

---

668 Vgl. hierzu *König,* S. 285.

669 So *Riegel,* Computer und Recht 1986, S. 352.

670 Vgl. KK-*Griesbaum,* § 161 Rn. 4; *Meyer-Goßner*, § 161 Rn. 1a.

671 Vgl. *König,* S. 261.

672 So *Baumann,* FS für Posser, S. 307; *König,* S. 285.

673 BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 123.

674 BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 123.

Rechtsgrundlagen „auch in einer Norm zusammengefasst werden", sofern die Kompetenzordnung und die Anforderungen der Normenklarheit beachtet wurden.[675] Da diese Voraussetzungen mit Blick auf den allgemeinen Charakter des § 161 I StPO nicht erfüllt sind, ist zusammen mit der Rechtsprechung bei der Übermittlung von Geheimdienstinformationen stets auch eine Beachtung der geheimdienstlichen Übermittlungsregeln zu fordern. Die vorliegende Arbeit folgt dementsprechend dem zweiten Modell. Bei einer Anfrageübermittlung sind damit stets die strengeren Voraussetzungen der Nachrichtendienstgesetze in den § 20 BVerfSchG, § 9 III BNDG, § 11 II MADG sowie §§ 4, 7 IV G10 zu berücksichtigen.[676]

c) Zwischenergebnis zu Übermittlungsregeln

Eine Übermittlung von Geheimdienstinformationen zu Strafverfolgungszwecken kann primär nur bei schweren beziehungsweise staatschutzrelevanten Delikten erfolgen. Im Bereich der Telekommunikationsdaten sieht das G10 in den §§ 4, 7 IV G10 zudem erhöhte Anforderungen vor, die jedoch aufgrund einer extensiven Verweisungstechnik zum Teil an Klarheit einbüßen. Im Übrigen müssen sowohl bei einer Eigeninitiativ- als auch bei einer Anfrageübermittlung stets die Voraussetzungen der § 20 BVerfSchG gegebenenfalls i.V.m. § 9 III BNDG, § 11 II MADG beachtet werden. Eine ausschließlich auf § 19 I BVerfSchG oder § 161 I StPO gestützte Informationsübermittlung zu repressiven Zwecken wird vorliegend abgelehnt.

4. Verwertung von Geheimdienstinformationen

Die Verwertbarkeit nachrichtendienstlicher Erkenntnisse ist noch weitgehend ungeklärt.[677] Wie bereits im Rahmen der allgemeinen Grenzen dargestellt, unterliegt die repressive Nutzung von Geheimdienstinformationen sowohl systembedingten als auch verfassungsrechtlichen Grenzen. Diese sind in Form von Verwendungs- und Verwertungsregeln zu berücksichtigen.[678] Die nachfolgende Darstellung setzt sich mit den allgemeinen und speziellen Verwendungs- und Verwertungsregeln sowie der Berücksichtigung möglicher Fehler auseinander.

---

[675] BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 123.

[676] So auch SK-StPO-*Wohlers,* § 161 Rn. 31. Ebenso wohl BT-Drs. 14/5655, S. 21, in Bezug auf G10-Daten. Eine vergleichbare Begrenzung auf bestimmte Straftaten fordert auch *Hefendehl,* GA 2011, S. 229.

[677] So *Rehbein,* S. 240. Für eine Verwertbarkeit *Droste,* Handbuch, S. 588. A.A. bei *Gusy,* ZRP 1987, S. 50, der Vorfelderkenntnisse allein den Nachrichtendiensten vorbehalten möchte. Eine Zwischenlösung findet sich bei *Hefendehl,* GA 2011, S. 220ff.

[678] Die Verwendungs- bzw. Übernahmeregeln betreffen die zweite Tür des beschriebenen Zwei-Türen-Modells, vgl. *Bertram,* S. 308ff; *König,* S. 259.

a) Allgemeine Verwendungs- und Verwertungsregeln

Die vorliegend relevanten Verwendungs- und Verwertungsregeln finden sich in § 161 I, II StPO.

aa) Vorgaben des § 161 II StPO

Erster Anknüpfungspunkt für eine strafprozessuale Nutzung von Geheimdienstinformationen ist die spezielle Verwendungsregel des § 161 II StPO. Diese in Absatz 2 gefundene Regelung wurde erst mit Wirkung zum 1. Januar 2008 eingefügt und realisiert die Idee des sogenannten hypothetischen Ersatzeingriffs.[679] Inhaltlich regelt § 161 II StPO den Umgang mit personenbezogenen Daten, die von anderen Behörden als den Strafverfolgungsorganen erhoben wurden. Die Vorschrift ist damit auf Erkenntnisse der Dienste als „andere Behörden" anwendbar.[680] Die Verwendung zu Beweiszwecken setzt nach § 161 II StPO voraus, dass

- personenbezogene Daten aufgrund einer Maßnahme nach einem anderen Gesetz als der StPO erlangt wurden und
- die Maßnahme nach der StPO nur bei Verdacht bestimmter Straftaten zulässig gewesen wäre.

Sind diese Voraussetzungen erfüllt, gestattet § 161 II StPO die Verwendung entsprechender Daten zu Beweiszwecken, wenn

- die betroffene Person ihre Einwilligung erteilt (Variante 1) oder
- eine solche Maßnahme auch nach der StPO hätte angeordnet werden können (Variante 2).[681]

Der Anwendungsbereich der Norm ist auf personenbezogene Daten begrenzt. Diese müssen aus Ermittlungsmaßnahmen stammen, bei denen der Gesetzgeber den Verdacht einer bestimmten Straftat fordert. Die Verknüpfung der Ermittlungsermächtigungen an einen objektiv eingegrenzten Kreis von Straftaten ist üblicherweise ein Beleg für die generelle Eingriffsintensität entsprechender Maßnahmen.[682] Den objektiven Bezug stellt der Gesetzgeber hierbei regelmäßig durch die Begrenzung auf einen konkreten, abschließenden Straftatkatalog oder eine anderweitige

---

[679] Die Neuregelung geht auf das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der RL 2006/24/EG (BGBl. I, 2007, S. 3198) zurück; vgl. BT-Drs. 16/5846, S. 64. Die Einführung dieses Instituts wurde bereits im Jahre 2000 in Bezug auf die Nutzung präventiv polizeilicher Daten diskutiert, letztlich jedoch abgelehnt; vgl. BT-Drs. 14/2886, S. 3. Vertiefend KK-*Griesbaum,* § 161 Rn. 35; *Hefendehl,* GA 2011, S. 220ff; Radtke/Hohmann-*Kretschmer,* § 161 Rn. 14; SK-StPO-*Wohlers,* § 161 Rn. 51.

[680] Vgl. BT-Drs. 16/5846, S. 64; *Rehbein,* S. 230.

[681] Vertiefend *Rehbein,* S. 230ff; *Singelnstein,* ZStW 120 (2008), S. 876ff.

[682] Vgl. *Eisenberg,* Rn. 358; *Singelnstein,* ZStW 120 (2008), S. 876.

nähere Umschreibung her.[683] Eine solche Umschreibung kann beispielsweise durch eine Festlegung auf Verbrechen, Taten von erheblicher Bedeutung oder die Verknüpfung mit einer bestimmten Begehungsform erfolgen.[684] Erfasst sind demnach Erkenntnisse, die aus Maßnahmen wie denen nach §§ 98a, 99, 100a, 100c, 100f, 100h, 100i, 110a, 111, 131 III, 131a III, 131b, 163d, 163e, 163f StPO stammen. Hierbei handelt es sich primär um heimliche Ermittlungsmaßnahmen.[685] Sind diese strafprozessualen Erhebungsmaßnahmen nur bei bestimmten, schwerwiegenden Sachverhalten erlaubt, sollen diese Wertungen nach den Vorgaben des § 161 II StPO auch bei einer außerstrafprozessualen Erhebung berücksichtigt werden.[686] Insofern dürfen die Anforderungen an eine Zweckumwidmung nicht unter diejenigen strafprozessualen Vorgaben abgesenkt werden, die bei einer originären strafprozessualen Erhebung gegolten hätten.[687] In dieser Auslegung gewährleistet § 161 II StPO eine auf das Schutzniveau des Strafverfahrens abgestimmte Beweisverwertung.[688]

Ist der Anwendungsbereich des § 161 II StPO eröffnet, muss der Richter im Zeitpunkt der Zweckumwidmung die Voraussetzungen des hypothetischen Ersatzeingriffs prüfen.[689] Zu diesem Zweck muss er untersuchen, ob die Strafverfolgungsbehörden zur Vornahme einer vergleichbaren Ermittlungsmaßnahme ermächtigt gewesen wären.[690] Dieser Prüfung liegt eine konkrete *ex post*-Betrachtung zugrunde.[691] Um eine Umgehung strafprozessualer Vorschriften zu verhindern, müssen bei einer Nachstellung der hypothetischen Ermittlungssituation damit sämtliche Voraussetzungen der hypothetisch einschlägigen Strafprozessnorm vorlie-

---

683 Vgl. BT-Drs. 16/5846, S. 58. Ähnlich *Hefendehl,* GA 2011, S. 225; *Rehbein,* S. 231.

684 So *Singelnstein,* ZStW 120 (2008), S. 879.

685 So *Singelnstein,* ZStW 120 (2008), S. 879, demzufolge nur die § 99 und § 100h I Nr. 1 StPO keine Heimlichkeit erfordern. Zur Eingrenzung auf heimliche Maßnahmen *Rehbein,* S. 232.

686 Allgemein zur Bindung an die ursprüngliche gesetzgeberische Wertung KK-*Griesbaum,* § 161 Rn. 35. Zur Bindung an Erhebungszweck BVerfG NJW 2000, S. 55, 64; BVerfG NJW 2004, S. 999, 1018f.

687 Vgl. *Singelnstein,* ZStW 120 (2008), S. 882.

688 Vgl. *Knieriem,* StV 2008, S. 601; *Puschke/Singelnstein,* NJW 2008, S. 117; *Glaser/Gedeon,* GA 2007, S. 435. Dem widerspricht *Rehbein,* S. 250, die dem § 161 II StPO allerdings eine andere Auslegung zugrunde legt.

689 Vgl. *Rehbein,* S. 235, sowie ausführlich *Singelnstein,* ZStW 120 (2008), S. 880ff. Nach *Singelnstein* müssen die Voraussetzungen des hypothetischen Ersatzeingriffs jedoch nicht nur bei der Zweckumwidmung, sondern bis zum Abschluss des Verfahrens vorliegen, sodass der Richter ständig deren Fortbestehen prüfen müsste.

690 Vgl. zu dieser insgesamt umstrittenen Ansicht *Allgayer/Klein,* wistra 2010, S. 132; *Eisenberg,* Rn. 358. Ähnlich *Hefendehl,* GA 2011, S. 225.

691 So *Singelnstein,* ZStW 120 (2008), S. 881. Die Gegenansicht stellt allein auf die Art der Maßnahme und nicht die einzelnen Eingriffsvoraussetzungen ab, vgl. hierzu KK-*Griesbaum,* § 161 Rn. 35, und *Rehbein,* S. 235, 237.

gen.[692] Der hypothetische Ersatzeingriff kann damit je nach Ermächtigungsgrundlage neben dem Vorliegen einer tauglichen Straftat zusätzlich etwa den Nachweis der besonderen Tatschwere oder die Einhaltung von Subsidiaritätsklauseln erforderlich machen.[693] Erkenntnisse aus dem Einsatz eines IMSI-Catchers nach § 9 IV BVerfSchG sind in diesem Sinne beispielsweise an § 100i StPO i.V.m. § 100a II StPO zu messen. Für eine Verwendung von Daten einer akustischen Wohnraumüberwachung nach § 9 II BVerfSchG müssten demgegenüber die in § 100c StPO genannten Voraussetzungen beachtet werden.[694]

Schwierigkeiten ergeben sich allerdings bei einer Spontanübermittlung, wenn aufseiten der Strafverfolgungsbehörden bislang noch kein Anfangsverdacht vorlag.[695] Prüft man unter Zugrundelegung eines hypothetischen Sachverhalts die Voraussetzungen der strafprozessualen Ermächtigungsgrundlage, müsste die Verwendbarkeit aufgrund des fehlenden Anfangsverdachts abgelehnt werden.[696] Da der Anfangsverdacht erst durch die Übermittlung begründet wird, müsste die hypothetische Nachstellbarkeit verneint werden. Gegen einen derart reduzierten Anwendungsbereich sprechen jedoch die Existenz der Übermittlungsregelungen sowie das darin zum Ausdruck kommende Strafverfolgungsinteresse. Das in Bezug auf den hypothetischen Ersatzeingriff fehlende Merkmal muss in diesen Fällen fingiert werden. Diese Fiktion ist jedoch angesichts des überwiegenden Strafverfolgungsinteresses im Bereich der Schwerstkriminalität zu akzeptieren, zumal die Übermittlungsvorschriften ihrerseits eine dem Anfangsverdacht angenäherte Übermittlungsschwelle voraussetzen.

Sind die übrigen Voraussetzungen des § 161 II StPO erfüllt, sind die Erkenntnisse in beweisrechtlicher Hinsicht grundsätzlich frei verwertbar.[697] Die allgemeine Verwertungsbefugnis kann in Bezug auf nachrichtendienstliche Erkenntnisse neben der Aufklärungspflicht nach § 244 II StPO i.V.m. der freien Beweiswürdigung nach § 261 StPO zudem auf die Existenz der Verwendungsregeln selbst gestützt werden, welche zugleich eine Befugnis zur späteren Beweisverwertung beinhal-

---

692 Hierzu ist ein konkreter Prüfungsmaßstab besser geeignet als eine abstrakte Betrachtung; vgl. BVerfGE 109, 279, 377, sowie *Allgayer/Klein,* wistra 2010, S. 132; *Singelnstein,* ZStW 120 (2008), S. 881.

693 So *Singelnstein,* ZStW 120 (2008), S. 882.

694 Ein Anwendungsbeispiel findet sich bei *Knieriem,* StV 2008, S. 601. Insgesamt kritisch *Hefendehl,* GA 2011, S. 226.

695 Für die Anfrageübermittlung nach § 161 I StPO ergebe dies keine Schwierigkeiten, da ein Ersuchen bereits das Bestehen eines Anfangsverdachts voraussetzt.

696 Unter Verweis auf die Gefahr eines Zirkelschlusses etwa *Kelnhofer/Krug,* StV 2008, S. 666; *Ostendorf,* ZIS 2010, S. 306; *Singelnstein,* ZStW 120 (2008), S. 882.

697 Vgl. *Rehbein,* S. 144.

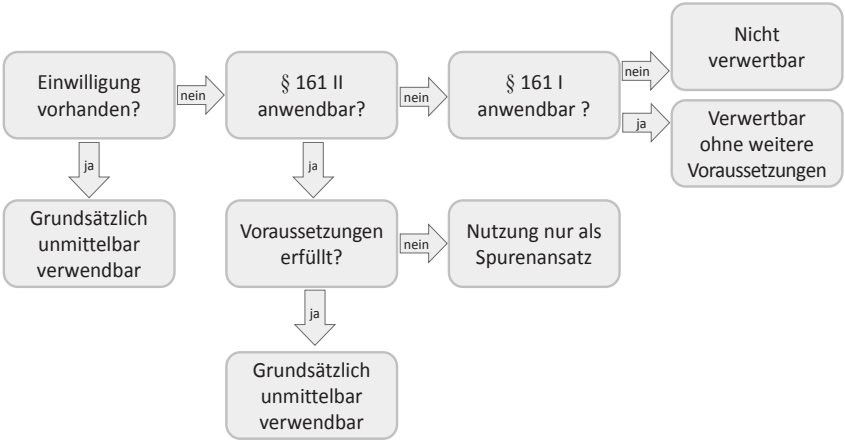

Abbildung 3: Verwertungspfad im Rahmen von § 161 II, I StPO

ten.[698] Inhaltlich ist die unmittelbare Verwertung nach den Vorgaben der Zweckbindung nur hinsichtlich der in den Übermittlungsvorschriften genannten Delikte zulässig.[699] Zwar enthält § 20 BverfSchG, anders als etwa § 19 I 2 BverfSchG, keine ausdrückliche Bindung des Empfängers an den Übermittlungszweck, die für eine Zweckänderung erforderliche Vereinbarkeit von Erhebungs- und späterem Verwendungszweck ist jedoch nur gegeben, wenn diese bei der späteren Verwendung tatsächlich eingehalten wird. In diesem Sinne sollen staatsschutzrelevante Erkenntnisse gerade nicht zur Verfolgung eines einfachen Diebstahls eingesetzt werden können. Sind die Voraussetzungen des § 161 II StPO nicht erfüllt, scheidet eine Verwendung zu Beweiszwecken ohne Einwilligung des Betroffenen aus. Eine solche wird der Angeklagte regelmäßig nur abgeben, wenn sich die Erkenntnisse zu seinen Gunsten auswirken.

Bei einer Beurteilung des § 161 II StPO ist weiterhin zu berücksichtigen, dass die Verwendung nach dem ausdrücklichen Wortlaut von vorneherein auf die unmittelbare Beweisverwertung beschränkt ist.[700] Eine mittelbare Nutzung außerstraf-

---

[698] Vgl. allgemein zur Verwertungsbefugnis *Grawe,* S. 188f; *Rehbein,* S. 144f; *G. Walter,* S. 283.

[699] Vgl. hierzu Löwe/Rosenberg-*Erb,* § 161 Rn. 82. Ebenso *Hefendehl,* GA 2011, S. 229, der eine Bindung an die konkreten Übermittlungsdelikte fordert. Denkbar wäre allerdings auch eine abstrakte Festlegung auf die im Katalog genannten Straftaten, da der Gesetzgeber bei diesen Delikten von einem erhöhten Strafverfolgungsinteresse ausgeht.

[700] Daher spricht der Wortlaut von einer Verwendung zu Beweiszwecken; vgl. BT-Drs. 16/5846, S. 64; *Bertram,* S. 230; *Joecks*, § 161 Rn. 12aff. Ist bereits der Anwendungsbereich des § 161 II StPO nicht eröffnet, gilt § 161 I StPO.

prozessual erhobener Erkenntnisse wird nicht ausgeschlossen, sondern vom Gesetzgeber explizit erlaubt.[701] Dieser folgt damit der umstrittenen Rechtsprechungspraxis, welche die Nutzung von Erkenntnissen als Spurenansatz unabhängig vom Erhebungskontext gestattet.[702] Die im geheimdienstlichen Kontext erhobenen Erkenntnisse können folglich unbegrenzt als Spurenansatz für weitere Ermittlungen herangezogen werden.[703]

Im Ergebnis schränkt die Vorschrift des § 161 II StPO die Verwendung nachrichtendienstlicher Erkenntnisse zu Beweiszwecken für generell eingriffsintensive Maßnahmen ein. Die Nutzung als Spurenansatz unterliegt keinen speziellen Beschränkungen.

bb) Vorgaben des § 161 I StPO

Außerhalb des Anwendungsbereichs des § 161 II StPO können geheimdienstliche Erkenntnisse höchstens unter den Voraussetzungen des § 161 I StPO Eingang in ein Strafverfahren finden. Die Generalklausel des § 161 I StPO gestattet den Strafverfolgungsbehörden in diesem Zusammenhang unter anderem Auskünfte einzuholen sowie entsprechende Erkenntnisse entgegenzunehmen.[704] Voraussetzung sind lediglich ein aktuell bestehender Anfangsverdacht und die Erforderlichkeit für die Strafverfolgung.[705] Dieses umfassende Zugriffsrecht wird als Annex durch eine allgemeine Verwertungsbefugnis ergänzt.[706] § 161 I StPO kann aufgrund seiner Generalität jedoch nur Maßnahmen mit geringer Eingriffsintensität

---

[701] Kritisch dazu *Hefendehl,* GA 2011, S. 224f.

[702] So *Singelnstein,* ZStW 120 (2008), S. 885. Vgl. zum Streitstand KK-*Griesbaum,* § 161 Rn. 36; *Lohberger,* FS für Hanack, S. 264ff; *Meyer-Goßner*, § 477 Rn. 6. Stellvertretend für die Rechtsprechung vgl. BGHSt 27, 355, 1. Leitsatz, sowie BGH NStZ 1998, S. 426.

[703] Vgl. *Allgayer/Klein,* wistra 2010, S. 130f; *Bertram,* S. 230; *Meyer-Goßner*, § 161 Rn. 18b, 18c in Anknüpfung an die Rechtsprechung des BVerfG in NJW 2005, 2766; vgl. auch *Joecks*, § 161 Rn. 12a ff. Die Heranziehung als Spurenansatz beinhaltet die Nutzung der Information zum Auffinden weiterer, verwertbarer Beweismittel; vgl. insgesamt Abb. 3.

[704] Im Jahr 2000 wurde die Aufgabenzuweisungsnorm in eine Ermittlungsgeneralklausel umgestaltet, vgl. BT-Drs. 14/1484, S. 16, 23; KK-*Griesbaum*, § 161 Rn.1; Löwe/Rosenberg-*Erb,* § 161 Rn. 2.

[705] Vgl. *Grawe,* S. 281; *Zöller,* in: Roggan/Kutscha, S. 501.

[706] Vgl. *Grawe,* S. 281f. Im Umkehrschluss zu § 161 II StPO sei in den nicht erfassten Fällen von einer generellen Verwendbarkeit auszugehen. Zugleich unter Verweis auf die gescheiterte Einführung einer Verwendungsregel in den 1990er Jahren infolge des Urteils des BGH NStZ 1992, S. 44f BT-Drs. 14/2886, S. 3. Wenig später wurde in einem weiteren Gesetzesentwurf zudem ausdrücklich die Fortgeltung der sonstigen Verwertungsregelungen festgestellt, vgl. BT-Drs. 14/1484, S. 23.

rechtfertigen.[707] Diese Grundsätze müssen einheitlich sowohl für die Informationserhebung als auch für die vorliegend relevante Nutzung entgegengenommener Erkenntnisse gelten. Dieses Ergebnis wird durch verfassungsrechtliche Erwägungen gestützt. Die Beweisverwertung außerstrafprozessual erhobener Erkenntnisse kann aufgrund der damit verbundenen Zweckänderung mit einem Grundrechtseingriff verbunden sein, dessen Rechtfertigung den verfassungsrechtlichen Anforderungen an die Verhältnismäßigkeit und hinreichende Bestimmtheit genügen muss.[708] Diese Anforderungen steigen mit zunehmender Eingriffstiefe beziehungsweise -intensität.[709] Da die Vorschrift des § 161 I StPO weder in Bezug auf Art und Umfang noch auf die Sensibilität der Datenerhebung Konkretisierungen vorsieht, scheidet die Verwertung von Geheimdienstinformationen auf der Grundlage des § 161 I StPO regelmäßig aus.[710] Sie kommt lediglich bei nicht-personenbezogenen Daten oder Bagatellinformationen sowie bei Erkenntnissen in Betracht, die aus geringfügigen Eingriffen stammen.[711] Sobald die Maßnahmen eine gewisse Grundrechtsrelevanz aufweisen, kann die Generalklausel eine zweckändernde Übernahme von Geheimdienstinformationen nicht mehr rechtfertigen.[712] Maßnahmen, die zwar nicht generell, dafür aber im Einzelfall eine besondere Eingriffsintensität erreichen, können damit nicht über § 161 I StPO eingeführt werden. Eine solche Eingriffsintensität im Einzelfall kann aus einer Involvierung Dritter, einer Kumulation verschiedener Informationseingriffe oder dem besonderen Umfang der Datenerhebung resultieren.[713]

b) Spezialgesetzliche Beschränkungen

Diese allgemeinen Verwendungs- und Verwertungsregeln werden durch spezialgesetzliche Vorgaben der Nachrichtendienstgesetze und des G10 ergänzt. In den einzelnen Ermächtigungsgrundlagen finden sich dementsprechend verschiedene

---

[707] Vgl. BT-Drs. 14/1484, S. 23; BVerfG NJW 2009, S. 1405, 1407; *P.-A. Albrecht,* StV 2001, S. 419; *Hefendehl,* GA 2011, S. 222.

[708] Vgl. *Grawe,* S. 282; *Rehbein,* S. 143ff. Bei einer rein strafprozessualen Erhebung scheidet ein selbstständiger Grundrechtseingriff durch die Verwertung mangels Zweckänderung aus. Die Verwertungsbefugnis ist bereits in der ursprünglichen Erhebungsnorm enthalten. Diese wäre sonst zur Aufgabenerfüllung von vorneherein ungeeignet.

[709] Vgl. Maunz/Dürig-*Di Fabio,* Art. 2 Rn. 182; *Singelnstein,* ZStW 120 (2008), S. 875. So auch BVerfG NJW 2009, S. 1405, 1407, das eine hohe Eingriffsintensität insbesondere bei Verdachtslosigkeit und großer Streubreite von Erhebungsmaßnahmen annimmt.

[710] Allgemein kritisch zu § 161 I StPO *Hefendehl,* GA 2011, S. 223.

[711] Sinngemäß BVerfG NJW 2009, S. 1405, 1407; *Grawe,* S. 176, 282; Löwe/Rosenberg-*Erb,* § 161 Rn. 2; *Hefendehl,* GA 2011, S. 222; *Zöller,* in: Roggan/Kutscha, S. 502. *Hefendehl* kritisiert, dass diese Vorgaben nicht immer eingehalten werden.

[712] So *Grawe,* S. 282.

[713] Vgl. hierzu *Singelnstein,* ZStW 120 (2008), S. 876.

Verwendungsvorgaben[714] sowie Vorschriften zum Schutz des Kernbereichs der privaten Lebensgestaltung,[715] zeugnisverweigerungsberechtigter Personen[716] oder Daten Dritter.[717] Zudem finden sich für bestimmte Ermittlungsmethoden zum Teil ausdrückliche Verwendungsregeln. Daten aus einem besonderen Auskunftsverlangen nach § 8a BVerfSchG können beispielsweise nach § 8b II 6 BVerfSchG einem absoluten Verwendungsverbot unterliegen, wenn die G10-Kommission diese für unzulässig oder nicht notwendig erklärt. In diesem Fall unterliegen die Daten einem absoluten Verwendungsverbot und sind unverzüglich zu löschen.

c) Berücksichtigung von Fehlern

Mängel im geheimdienstlichen Erhebungs- und Übermittlungsprozess können einer Verwertung von Geheimdienstinformationen entgegenstehen. Die Nachrichtendienste treten bei einer Übermittlung an den Strafverfolgungssektor nicht als unbeteiligter Anzeigeerstatter auf, sondern sind dem Staat zuzurechnen.[718] Verstöße gegen nachrichtendienstliche Ermächtigungsgrundlagen können daher, ebenso wie die Verstöße anderer Ermittlungsbehörden, bei der Beweisverwertung berücksichtigt werden.[719] Sie unterliegen im Grundsatz einer vollumfänglichen gerichtlichen Kontrolle.[720] Die nachfolgenden Ausführungen geben einen Überblick über die zentralen Fehlerquellen im Geheimdienstsektor und deren Auswirkungen auf die Beweisverwertung.

aa) Eingriffe in den Kernbereich privater Lebensgestaltung

Konsequenzen für die Beweisverwertung sind vor allem bei Grundrechtseingriffen in den Wesensgehalt i.S.d. Art. 19 II GG oder den Menschenwürdekern i.S.d. Art. 1 I GG denkbar.[721] Bei der Gewinnung von Geheimdienstinformationen kom-

---

[714] So etwa in §§ 9 II, 12 IV, 19 I, III, IV, 22a BVerfSchG sowie §§ 4 II, 6 II G10.

[715] Vgl. §§ 3a, 5a G10.

[716] Vgl. § 3b G10.

[717] Vgl. etwa §§ 4 V, 6 V G10 oder § 9 IV 6 BVerfSchG.

[718] So u.a. *Rehbein,* S. 184f.

[719] Die durch das Trennungsgebot bedingte Aufteilung in geheimdienstliche und repressive Tätigkeiten darf sich nicht zulasten des Bürgers auswirken.

[720] Vgl. *Rehbein,* S. 185ff. In dieser Hinsicht wurde u.a. das Merkmal der „tatsächlichen Anhaltspunkte“ für voll überprüfbar erklärt, vgl. BVerwG NJW 1991, S. 581, 2. Leitsatz. Die Überprüfbarkeit wird u.a. durch die umfassenden Protokollierungspflichten ermöglicht. Zur allgemeinen Überprüfbarkeit unbestimmter Rechtsbegriffe BVerfG NJW 1984, S. 33, 35; NJW 1991, S. 2005f; NJW 2001, S. 1121, 1123.

[721] Vgl. *Eisenberg*, Rn. 386. Ein selbstständiges Verwertungsverbot nachrichtendienstlicher Erkenntnisse ist abzulehnen. Dieses wird zum Teil wegen des Vorfeldbezugs nachrichtendienstlicher Beobachtungen diskutiert, vgl. *Rehbein,* S. 237ff, 257. Dieser Streit-

men derartige Informationseingriffe vor allem bei Daten aus dem Kernbereich privater Lebensgestaltung in Betracht. In den Nachrichtendienstgesetzen wird deren Schutz ausdrücklich oder vermittelt über den Verhältnismäßigkeitsgrundsatz gewährleistet.[722] Die Umsetzung dieses Schutzes erfolgt durch entsprechende Erhebungs- und Speicherungsverbote sowie Löschungspflichten. Kommt es trotz dieser Schutzvorkehrungen zu einem kernbereichsrelevanten Vorgang, sind die Kriterien der oben dargestellten Sphärentheorie uneingeschränkt anzuwenden. Eingriffe in die Intimsphäre führen damit ungeachtet des geheimdienstlichen Erhebungskontextes zu einem absoluten Verwertungsverbot.[723]

Die Entscheidung für einen unantastbaren Bereich privater Lebensgestaltung wird jedoch durch eine zum Teil ergebnisorientierte Rechtsprechungspraxis relativiert. Insbesondere in Fällen schwerer Kriminalität hat der BGH vereinzelt eine Zuordnung zum absolut geschützten Kernbereich abgelehnt und damit die Möglichkeit einer Abwägung und damit Verwertung eröffnet.[724] Diese Praxis ist für die Nutzung von Geheimdienstinformationen von unmittelbarer Relevanz, da die Nachrichtendienstgesetze den Umfang der übermittlungstauglichen Geheimdienstinformationen von vorneherein auf schwerwiegende Delikte beschränken. Vor diesem Hintergrund wäre es daher nicht verwunderlich, wenn die Rechtsprechung die Kernbereichstheorie bei einer Nutzung von Geheimdienstinformationen teilweise ebenfalls preisgegeben würde. Die zu dieser Problematik ergangene Rechtsprechung zeichnet sich jedoch durch keine einheitliche Linie aus, sodass eine abschließende Bewertung vorliegend nicht möglich ist. Sicher ist nur, dass bei der Nutzung von Geheimdienstinformationen die dogmatische Unterscheidung zwischen dem unantastbaren Kernbereich und dem relativ geschützten Abwägungsbereich durch die Rechtsprechungspraxis erheblich erschwert wird.

bb) Selektive Datenerhebung

Bei einer strafprozessualen Nutzung von Geheimdienstinformationen müssen zudem die Gefahren einer selektiven Datenerhebung berücksichtigt werden. Anders als die Staatsanwaltschaften sind die Geheimdienste nicht verpflichtet, die Informationserhebung gleichermaßen auf belastende und entlastende Tatsachen zu richten. Die Datenbestände der Dienste durchlaufen insofern einen anderen Selektionsprozess, als dies bei einer strafprozessualen Beweiserhebung der Fall

---

stand ist aufgrund der vorliegend favorisierten konkreten Betrachtungsweise nicht übertragbar.

722 Vgl. u.a. § 3a G10; §§ 8 V, 9 I 2, 3 BVerfSchG.

723 Vgl. allgemein BVerfG NJW 1990, S. 563f; BVerfG NJW 2004, S. 999, 1002; *Eisenberg,* Rn. 387; *Hefendehl,* GA 2011, S. 230.

724 Vgl. BGH NJW 1988, S. 1037, 1038; BGHSt 19, 331; *Herrmann,* FS für Jescheck, S. 1293; *Roxin/Schünemann,* § 24 Rn. 56; *Trüg,* S. 297.

wäre.[725] Zwar sind die Strafverfolgungsbehörden nach Erhalt der Informationen ihrerseits zur Vornahme eigenständiger Ermittlungen verpflichtet und können dadurch die Ermittlungserkenntnisse um entlastende Informationen ergänzen, aufgrund der zunächst bruchstückhaften beziehungsweise vorselektierten Informationslage besteht jedoch weiterhin die Gefahr einer verzerrten Sachverhaltsdarstellung.[726] Derart bewusst oder unbewusst verkürzte Sachverhalte können durch die Regelungen des Strafverfahrensrechts jedoch hinreichend berücksichtigt werden. Dies wird am Beispiel der klassischen Zeugenaussage deutlich. Der Zeuge gibt in der Zeugenvernehmung seine Wahrnehmung ebenfalls nur selektiv beziehungsweise persönlich eingefärbt wieder.[727] Die damit verbundenen Unsicherheiten führen jedoch nicht automatisch zur völligen Untauglichkeit des Beweismittels, sondern mindern lediglich dessen Beweiswert. Dieser Gedanke ist auf die Nutzung von Geheimdienstinformationen übertragbar. Demnach muss der Richter die mit der Nutzung von Geheimdienstinformationen verbundenen Unsicherheiten bei der Beurteilung des Beweiswerts berücksichtigen.[728]

cc) Verzerrungen durch nachrichtendienstliche Analysen

Weitere Bedenken werden in Bezug auf die Berücksichtigung nachrichtendienstlicher Analysen geäußert. Nach § 3 I BVerfSchG obliegt den Diensten neben der Erhebung zusätzlich die „Auswertung von Informationen". Diese nachrichtendienstliche Bewertung wird üblicherweise mit übermittelt. Da das Gericht aus tatsächlichen Gründen oftmals nicht in der Lage ist die Korrektheit dieser nachrichtendienstlichen Analyse zu überprüfen, wird zum Teil eine unzulässige Beeinflussung der Richter befürchtet.[729] Allerdings wird diese Problematik durch eine erweiterte Übermittlungspflicht zumindest teilweise abgemildert. Danach darf sich die Übermittlung nicht nur auf die aufbereiteten Informationen begrenzen, sondern muss sämtliche Tatsachen erfassen, die der Bewertung zugrunde liegen.[730] Dennoch verbleibende Unsicherheiten muss das Gericht bei der Würdigung der Beweise ausgleichen.

---

[725] Vgl. *Hefendehl,* GA 2011, S. 226. Zur Selektivität der Datenerhebung und -weitergabe vgl. auch *Rehbein,* S. 259ff.

[726] In diesem Sinne *Griesbaum,* FS für Nehm, S. 135.

[727] Insofern kritisch *Rehbein,* S. 262.

[728] Vgl. *Rehbein,* S. 263.

[729] Vgl. *Droste,* Handbuch, S. 475; *Gusy,* NVwZ 1983, S. 327; Miebach-*Lampe/Hegmann,* Vor §§ 93 ff Rn. 35; *Roggan,* in: Roggan/Kutscha, S. 424. Als Beispiel wird u.a. das *Schmücker*-Verfahren genannt, vgl. *Ferse,* KritV 1994, S. 260. Generell zu den Möglichkeiten, den Wahrheitsgehalt nachrichtendienstlicher Erkenntnisse zu überprüfen, *Rehbein,* S. 273.

[730] Vgl. *Droste,* Handbuch, S. 475; *Gusy,* NVwZ 1983, S. 327f; *Rehbein,* S. 273. Zu den Problemen bei der Weitergabe *Schneider,* NJW 1978, S. 1602f.

dd) Rechtswidrige Erhebung

Die beweisrechtliche Berücksichtigung von Fehlern im geheimdienstlichen Erhebungsprozess ist weitgehend ungeklärt. Einigkeit besteht lediglich in Bezug auf allgemeine Grenzen, wie die Willkürgrenze. Nach dieser führt die schwerwiegende oder bewusste Verkennung gesetzlicher Vorgaben zu einem Beweisverwertungsverbot.[731] Dem steht der Fall gleich, dass gänzlich ohne Rechtsgrundlage gehandelt wird.[732] Diese Grundsätze sind Ausdruck eines allgemeinen Rechtsverständnisses und kommen ungeachtet der spezifischen Besonderheiten des Geheimdienstsektors zur Anwendung. Dementsprechend führt eine bewusst rechtswidrige Erhebung oder Übermittlung zur Unverwertbarkeit der übermittelten Geheimdienstinformationen.[733] Gleiches muss gelten, wenn die Beteiligung der Dienste selbst wissentlich verheimlicht wird.[734]

Abseits der Willkürgrenze ist unklar, ob und wie Fehler im geheimdienstlichen Erhebungsprozess bei der Beweisverwertung berücksichtigt werden können. Vorbedingung für eine Beweisverwertung ist zunächst die Einführung entsprechender Erkenntnisse in ein Strafverfahren. In diesem Zusammenhang wird bereits bezweifelt, ob rechtswidrig erhobene Geheimdienstinformationen überhaupt Gegenstand einer Zweckentfremdung sein können oder nicht vielmehr von vorneherein einem Verwertungsverbot unterliegen.[735]

Die Rechtsprechung teilt etwaige Bedenken nicht, sondern erklärt die allgemeinen Grundsätze zu den relativen Beweisverwertungsverboten für anwendbar.[736] Zwar sei der Gesetzgeber vom Grundsatz der rechtmäßigen Erhebung ausgegangen, daraus könne jedoch kein Verwertungsverbot für rechtswidrige Daten gefolgert werden. Dieses Ergebnis gelte selbst mit Blick auf die verschiedenen strafprozessualen Verwendungsregeln. Diese Behauptung belegt der BGH unter Verweis auf die parallel zu § 161 II StPO formulierte Verwendungsregel des § 477 II 2 StPO im Bereich der präventiv-polizeilichen Daten. Würde man deren Anwendungsbereich von vorneherein auf rechtmäßig erhobene Erkenntnisse begrenzen, käme dies in Bezug auf rechtswidrig erhobene Daten einem generellen

---

731 Zu diesem Grundsatz zuletzt BVerfG NStZ 2011, S. 103, 105; ebenso BVerfG NJW 2006, S. 2684, 2686, sowie *Roggan,* in: Roggan/Kutscha, S. 420.

732 So *Rehbein,* S. 192f.

733 So etwa *Stahl/Demuth,* DStR 2008, S. 600f, zur Verwertbarkeit illegal erlangter Steuerdaten aus Liechtenstein. Sie plädieren für ein Beweisverwertungsverbot für den Fall, dass der BND die Daten unter gezieltem Einsatz von Geheimdienstmethoden erlangt hat, um hierdurch das „Ermittlungsrepertoire der Strafverfolgungsbehörden um nachrichtendienstliche Methoden" erweitern zu können.

734 So *Salditt,* FS für Schaumburg, S. 1280ff, der in diesem Fall von einer Steuerung des Ermittlungsrichters kraft überlegenen Wissens spricht.

735 Die Figur der hypothetischen Ermittlungsverläufe hilft in diesem Fall nicht weiter, da sie den Aspekt der Zweckänderung gerade nicht berücksichtigen kann.

736 Vgl. zu präventiv-polizeilichen Daten BGH NJW 2009, S. 3448, 3453.

Verwendungserbot gleich. Dieser Automatismus würde innerhalb des Strafverfahrens zu widersprüchlichen Ergebnissen führen. Danach könnten beispielsweise in einem Ausgangsverfahren rechtswidrige Daten unter Zugrundelegung der klassischen Abwägungslehre verwertet werden, während dieselben Daten für eine andere Tat desselben Täters aufgrund der Unzulässigkeit einer Zweckentfremdung einem Verwertungsverbot unterlägen. Allerdings hält der BGH ein Verwertungsverbot für möglich, wenn durch die Nutzung der rechtswidrigen Daten die Vorgaben der Verwendungsregel umgegangen werden.[737] In den übrigen Fällen bestimmt er die Annahme eines Verwertungsverbots nach den Umständen des Einzelfalls und damit anhand der allgemeinen Abwägungslösung. Inwiefern die Rechtsprechung die Berücksichtigung des Verwertungsverbots darüber hinaus von einem rechtzeitigen Widerspruch abhängig macht, ist nicht ersichtlich. Zwar erscheint die Anwendbarkeit der Widerspruchslösung aufgrund des besonderen Charakters der Verwendungsregeln eher unwahrscheinlich, dennoch empfiehlt sich bei einem Verfahrensfehler die vorsorgliche Einlegung eines entsprechenden Widerspruchs.[738]

In der Literatur wird diese Problematik weitaus kritischer gesehen. Zum Teil wird eine Zweckänderung rechtswidriger Geheimdienstinformationen generell für unzulässig gehalten. Nach dieser Ansicht ist eine Übermittlung von Geheimdienstinformationen von vorneherein auf Zufallsfunde zu beschränken, um einer Umgehung strafprozessualer Anordnungsvoraussetzungen vorzubeugen. Da Zufallsfunde nach dieser Ansicht per Definition nur bei einer rechtmäßigen Erhebung auftreten können, scheidet die Übermittlung und Verwertung rechtswidrig erhobener Geheimdienstinformationen automatisch aus.[739] Neben den Bedürfnissen des Trennungsgebots sei eine solche Begrenzung aus Rechtsschutzgründen zwingend erforderlich.[740] Aufgrund der Geheimhaltung nachrichtendienstlicher Vorgänge habe der Einzelne keine Möglichkeit, gegen den Rechtsverstoß vorzugehen.[741] Eine Verwertung der Erkenntnisse würde diesen Verstoß noch vertiefen und sei daher abzulehnen. Gelegentlich wird ergänzend auf die parallele Diskussion in anderen Sicherheitsbereichen verwiesen.[742] Werde dort zum Teil die zweckumwidmende

---

[737] BGH NJW 2009, S. 3448, 3454.

[738] So wurde in BGH StV 2001, S. 545, und BGH vom 12.7.2000 – 1 StR 113/00 die Notwendigkeit eines Widerspruchs bei der Verwertung von Zufallserkenntnissen sowie bei Ermittlungen ohne Anfangsverdacht bejaht. Zur vorsorglichen Einlegung eines Widerspruchs vgl. *Kuhn,* JA 2010, S. 891ff.

[739] Vgl. hierzu *Grawe,* S. 151; *Lohberger,* FS für Hanack, S. 259; *Rogall,* JZ 1996, S. 949. A.A. wohl Krekeler/Löffelmann-*Walther,* § 161 Rn. 27, allerdings zu präventivpolizeilichen Erkenntnissen.

[740] Vgl. *Albers,* S. 330; *Droste,* Handbuch, S. 475; *Gröpl,* S. 270; *Gusy,* ZRP 1987, S. 51. Zustimmend *Rogall,* ZStW 103 (1991), S. 929 Fn. 128.

[741] So *Gröpl,* S. 270.

[742] Vgl. KK-*Griesbaum,* § 161 Rn. 40; *Paeffgen,* FS für Hilger, S. 177 Fn. 17; *H. Wollweber,* NJW 2000, S. 3623. A.A. BVerfG NJW 2009, S. 3225; *Brodersen,* NJW 2000, S. 2539.

Verwendung präventiv-polizeilicher Daten auf rechtmäßig erhobene Erkenntnisse begrenzt, müsse diese Einschränkung erst Recht für eine Zweckumwidmung geheimdienstlicher Erkenntnisse gelten. Nach dieser Ansicht scheidet eine Verwertung rechtswidrig erlangter Nachrichtendienstdaten aufgrund eines absoluten Verwertungsverbots aus.[743]

Die von dieser Ansicht favorisierte generelle Annahme eines Verwertungsverbots setzt sich eingehend mit den Rechtsschutzinteressen des Betroffenen auseinander. Dieser Ansatz überdehnt jedoch das Merkmal des Zufallsfundes, indem unabhängig von der Art des Verstoßes pauschal von einem Verwertungsverbot ausgegangen wird. Allerdings sind geringfügige Fehler denkbar, bei denen die Annahme einer generellen Unverwertbarkeit ungerechtfertigt erscheint. In diesem Fall würde trotz fehlender Schutzwürdigkeit ein massiver Eingriff in die Strafrechtspflege gestattet werden. Der darüber hinaus angeführte Erst-Recht-Schluss in Bezug auf präventiv-polizeiliche Erkenntnisse ist nach der aktuellen Rechtsprechung zudem obsolet.[744]

Ein weiterer Ansatz hält demgegenüber eine zweckändernde Verwendung rechtswidriger Geheimdienstdaten grundsätzlich für zulässig. Diese Ansicht steht einer Zweckentfremdung rechtswidriger Informationen grundsätzlich offen gegenüber. Da die Nutzung rechtswidriger Daten allerdings viel tiefer in das Recht auf informationelle Selbstbestimmung eingreife, müsste der Gesetzgeber nach dieser Ansicht die erhöhte Eingriffsintensität in den maßgeblichen Rechtsgrundlagen ausreichend berücksichtigen.[745] Eine taugliche Ermächtigung müsste daher unter anderem die Zweckentfremdung rechtswidriger Daten strikt begrenzen.[746] Da die Vorschrift des § 161 StPO in ihrer derzeitigen Fassung diesen Anforderungen nicht genügt, könne sie die Zweckumwidmung rechtswidriger Geheimdienstinformationen nicht rechtfertigen.[747] Dieser Ansatz kommt damit ebenso wie die erste Ansicht

---

[743] Vgl. *Gröpl,* S. 270, 337; *Zöller,* in: Roggan/Kutscha, S. 502. Die von der Literatur favorisierte Unverwertbarkeit betrifft in ihrer Absolutheit lediglich eine Verwertung zulasten des Betroffenen. Demgegenüber müssen Fehler eine Verwertung zugunsten des Angeklagten nicht unbedingt ausschließen, sofern das Verwertungsverbot auf der Verletzung eines Rechtsguts beruht, über das der Betroffene die Verfügungsbefugnis besitzt. Vertiefend *Amelung,* StraFo 1999, S. 181ff; *Bertram,* S. 295; *Hamm,* StV 1998, S. 361ff; *Nack,* StV 1998, S. 366f*; Roxin/Schäfer/Widmaier,* StV 2006, S. 656.

[744] Vgl. hierzu BGH NJW 2009, S. 3448, 3453f.

[745] Vgl. *Singelnstein,* ZStW 120 (2008), S. 888. Allgemein zur Verwertung außerstrafprozessual erhobener Erkenntnisse SK-StPO-*Weßlau,* § 477 Rn. 13.

[746] Vgl. *Singelnstein,* ZStW 120 (2008), S. 888f. Zum Zweckentfremdungsverbot bei rechtswidrig erlangten Daten SK-StPO-*Weßlau,* § 477 Rn. 13; SK-StPO-*Wolter,* Vor § 151 Rn. 170. A.A. bei *Engelhart,* in: Wade/Maljević, S. 536, der zumindest bei schweren Straftaten von einer Verwertbarkeit ausgeht, ohne jedoch auf die erforderliche Bestimmtheit einzugehen.

[747] So zumindest *Singelnstein,* ZStW 120 (2008), S. 888f.

unabhängig vom konkreten Verstoß zur Unverwertbarkeit rechtswidriger Geheimdienstinformationen.[748]

Von der Rechtsprechung wird dieser Ansatz abgelehnt. Die Schaffung einer derartigen Rechtsgrundlage sei entbehrlich und der Verzicht darauf entspreche der üblichen Regelungstechnik des Gesetzgebers. Dieser habe, abgesehen von einzelnen Ausnahmen, auch sonst keine Bestimmungen geschaffen, die sich mit der Verwertung rechtswidriger Daten befassen.[749]

Selbst wenn man der Ansicht der Rechtsprechung zustimmen mag, so verdeutlicht der bisherige Meinungsstand jedoch erhebliche Unsicherheiten im Umgang mit der vorliegenden Materie. Es liegt insofern in der Verantwortung des Gesetzgebers die bisherige unklare Frage einer Zweckentfremdung von Geheimdienstinformationen durch die Schaffung einer eindeutigen beziehungsweise eindeutigeren Rechtsgrundlage zu beantworten.

In Bezug auf die beweisrechtliche Nutzung von rechtswidrigen Geheimdienstinformationen werden damit verschiedene Lösungsansätze vertreten. Lediglich bei einer Umgehung der Verwendungsbeschränkungen wird einheitlich die Möglichkeit eines Verwertungsverbots bejaht.[750]

Mit Blick auf die bisherige Rechtsprechungspraxis erscheint eine anhand der konkreten Fehlerquellen orientierte Abwägungslösung vorzugswürdig, sofern diese den Besonderheiten des Geheimdienstsektors ausreichend Rechnung trägt.[751] Fahrlässige Verfahrens- und Formfehler weisen in diesem Sinne üblicherweise nicht die erforderliche Schwere auf, um ein Verwertungsverbot zu begründen.[752] Die Missachtung nachrichtendienstlicher Zuständigkeitsregeln oder Mitteilungspflichten reicht daher zur Begründung eines Verwertungsverbots regelmäßig nicht aus oder kann zumindest nachträglich geheilt werden.[753] Davon abgesehen sind aber durchaus Fälle denkbar, in denen Verfahrensfehler im Geheimdienstsektor zur Begründung eines Verwertungsverbots ausreichen. Von einer entsprechenden Beachtlichkeit ist etwa bei einer fahrlässigen Missachtung präventiver Kontrollinstanzen auszugehen.[754] Die im Geheimdienstsektor existierenden Vorabkontrollen sind aufgrund der Abschottung des Geheimdienstsektors unter Rechtsschutzgesichtspunkten von erheblicher Relevanz. Grundsätzlich soll der mit der Heimlichkeit der

---

[748] Vgl. *Eisenberg,* Rn. 358; KK-*Griesbaum,* § 161 Rn. 40; *Rogall,* FS für Kohlmann, S. 484; *Singelnstein,* ZStW 120 (2008), S. 889; SK-StPO-*Wohlers,* § 161 Rn. 52. Eine Übersicht über den Streitstand findet sich bei *Paeffgen,* FS für Hilger, S. 160 Fn. 31.

[749] So BGH NJW 2009, S. 3448, 3453.

[750] Vgl. BGH NJW 2009, S. 3448, 3454, der diese Frage im Übrigen offen lässt.

[751] Vertiefend zu den nachfolgenden Ausführungen *Rehbein,* S. 192ff.

[752] Vgl. *Rehbein,* S. 194.

[753] So *Rehbein,* S. 196.

[754] So *Rehbein,* S. 196.

Ermittlungsmaßnahmen verbundene Informationsvorsprung durch die Vorabkontrollen kompensiert werden. Ein Fehler in diesem Bereich kann durch ein späteres Verfahren nicht mehr ausgeglichen werden und ist daher lediglich durch die Annahme eines Verwertungsverbots kompensierbar. Gleiches gilt im Wesentlichen für eine fahrlässige Missachtung der Hinweispflicht nach § 8 IV BVerfSchG.[755] Zwar handelt es sich bei einer Datenerhebung nach § 8 IV BVerfSchG gerade nicht um eine Beschuldigtenvernehmung i.S.d. § 136 StPO, sodass der Betroffene auf seine Mitwirkungsfreiheit und nicht auf seine Selbstbelastungsfreiheit hingewiesen werde; die Tatsache, dass er nicht zu einer Mitwirkung gezwungen werden kann, verhindert jedoch nicht, dass er sich unter Umständen faktisch zu einer solchen Aussage gezwungen fühlt. Insofern hat Gesetzgeber in § 8 IV BVerfSchG die persönliche Freiheit des Betroffenen ausdrücklich höher eingestuft als das nachrichtendienstliche Aufklärungsinteresse. Ein Verwertungsverbot ist damit gerechtfertigt, wenn sich der Betroffene in Unkenntnis seiner Aussagefreiheit selbst belastet.[756] Im Bereich der materiellen Fehlerquellen wird man ebenfalls überwiegend von einer Beweiserheblichkeit und damit Unverwertbarkeit rechtswidriger Geheimdienstinformationen ausgehen können.[757] Der geheimdienstliche Beobachtungsauftrag rechtfertige sich nur angesichts der überragend wichtigen Schutzgüter. Werden bei einer Beobachtung nun wesentliche Erhebungsvoraussetzungen missachtet, fehlt die maßgebliche Rechtfertigung für die Einräumung dieser spezifischen Erhebungsbefugnisse. In diesem Fall ist bereits aus Verhältnismäßigkeitsgesichtspunkten ein Verwertungsverbot erforderlich.[758] Bei einem Verstoß gegen nachrichtendienstliche Ermittlungsschwellen ergibt sich dies bereits aus einer Parallele zum Strafprozessrecht. Da dort die Missachtung des Anfangsverdachts zu einem Verwertungsverbot führt,[759] muss eine entsprechende Beschränkung erst Recht bei den noch viel niedrigeren nachrichtendienstlichen Ermittlungsgrenzen gelten.

Diese wenigen Beispiele verdeutlichen die Folgen, die verschiedene Fehler bei der geheimdienstlichen Informationserhebung für die Beweisverwertung haben können. Die Besonderheiten der geheimdienstlichen Informationserhebung führen nach der vorliegenden Lösung zur regelmäßigen Unverwertbarkeit rechtswidriger Geheimdienstinformationen. Allerdings kann durch die Möglichkeit einer Abwägung der unterschiedlichen Schwere der verschiedenen Fehlerquellen Rechnung getragen werden. Diese am konkreten Einzelfall orientierte Lösung ist am besten geeignet sowohl den Bedürfnissen der Strafverfolgung, den Besonderheiten des Geheimdienstsektors als auch dem Charakter der Verwendungsregeln gerecht zu werden.

---

755 Vgl. hierzu *Rehbein,* S. 199.

756 Vgl. *Rehbein,* S. 200.

757 Vgl. *Rehbein,* S. 201.

758 Vgl. zum G10 *Rehbein,* S. 201f.

759 Vgl. *Meyer-Goßner*, § 100a Rn. 35.

ee) Rechtswidrige Übermittlung

Weitere Fehler können aus einem Verstoß gegen die Übermittlungsvorschriften der § 20 BVerfSchG beziehungsweise §§ 4, 7 G10 resultieren. Mögliche Fehlerquellen sind beispielsweise die Übermittlung unter Missachtung der Straftatkataloge und des Verhältnismäßigkeitsgrundsatzes oder die Weiterleitung trotz bestehender Löschungspflichten beziehungsweise Übermittlungssperren. Zuständigkeitsfragen spielen in diesem Zusammenhang eine eher untergeordnete Rolle. Da innerhalb des Geheimdienstsektors selbst kaum Übermittlungsschranken bestehen, sind nur wenige Fälle denkbar, in denen ein Nachrichtendienst zu Unrecht über eine bestimmte Information verfügt.[760]

Bei der beweisrechtlichen Beurteilung von Übermittlungsfehlern sind erneut die Besonderheiten dieser Konstellation zu berücksichtigen.[761] Anders als im klassischen Ermittlungsverfahren werden vorliegend die maßgeblichen Informationen nicht durch die Strafverfolgungsbehörden, sondern durch die Geheimdienste erhoben. Insofern tritt bei einer unmittelbaren Nutzung die Informationsübermittlung an die Stelle der sonst erforderlichen strafprozessualen Beweiserhebung. Eine rechtswidrige Übermittlung ist damit in beweisrechtlicher Hinsicht mit einer rechtswidrigen Erhebung durch die Strafverfolgungsbehörden gleichzusetzen, sodass man für die Beurteilung eines Beweisverwertungsverbots von der Anwendbarkeit der allgemeinen Abwägungslehre ausgehen könnte. In diesem Fall wäre von einem Verwertungsverbot nur im Ausnahmefall, etwa bei bewussten oder grob fahrlässigen Übermittlungsfehlern, auszugehen.

Eine derart undifferenzierte Anwendung der Abwägungslehre steht allerdings im Widerspruch zum Grundsatz der Zweckbindung. Jeder Zweckänderung liegt eine Verhältnismäßigkeitsprüfung zugrunde, die den Umfang der zulässigen Verwendung auf den in der Übermittlungsvorschrift legitimierten Zweck limitiert.[762] Diese Begrenzung wird in den einzelnen Übermittlungsvorschriften zum Teil ausdrücklich betont.[763] Sie gestatten eine Zweckänderung nur unter den dort genannten Voraussetzungen. Außerhalb dieser Übermittlungsvoraussetzungen ist im Umkehrschluss eine Nutzung dieser Erkenntnisse umfassend ausgeschlossen.[764] Ein Verstoß gegen nachrichtendienstliche Verwendungsregeln setzt sich demnach auf strafprozessualer Ebene als Beweisverwertungsverbot fort. Darüber hinaus kann die Unverwertbarkeit rechtswidrig übermittelter Geheimdiensterkenntnisse auf einen Verstoß gegen das Trennungsgebot gestützt werden. Dieses ist bei einem Verstoß

---

760 So *Rehbein,* S. 204, die u.a. auf die Zentralstelleneigenschaft des BfV verweist.

761 Vgl. hierzu *Rehbein,* S. 184; *Singelnstein,* ZStW 120 (2008), S. 890.

762 Vgl. u.a. *Grawe,* S. 284.

763 So etwa in den §§ 7 VI 1 G10, 4 II, IV G10. Danach darf der Empfänger von G10-Daten diese nur im Rahmen des Übermittlungszwecks verwenden, vgl. *Rehbein,* S. 207.

764 Vgl. *Welp,* NStZ 1995, S. 604.

gegen die Übermittlungsvorschriften so gravierend verletzt, dass eine Beweisverwertung ausscheiden muss. Die Missachtung einer Übermittlungsvorschrift führt damit zu einem umfassenden Verwendungs- und damit Verwertungsverbot.[765] In diesem Fall ist sowohl eine Beweisverwertung als auch eine Nutzung der Erkenntnisse als Spurenansatz unzulässig.[766] Rechtswidrig übermittelte Geheimdienstinformationen dürfen damit nicht verwertet werden.[767]

ff) Fernwirkung

Eine gesonderte Auseinandersetzung ist hinsichtlich der Fernwirkung von Verwertungsverboten nachrichtendienstlicher Erkenntnisse erforderlich. Wie bereits im Rahmen der allgemeinen Ausführungen betont, wird im deutschen Strafverfahrensrecht eine Fernwirkung nur in Ausnahmefällen angenommen.

Dieses Regel-Ausnahme-Verhältnis gilt bei einer Nutzung nachrichtendienstlicher Erkenntnisse grundsätzlich in gleicher Weise. Aus dem Grundsatz der Zweckbindung ergeben sich insofern keine Besonderheiten, da die Fernwirkungsproblematik grundsätzlich die Verwertbarkeit mittelbar gewonnener Erkenntnisse betrifft. Die sich an eine Übermittlung anschließende Beweiserhebung erfolgt regelmäßig auf der Grundlage der StPO. Da die Strafverfolgungsbehörden diese zudem zu Strafverfolgungszwecken erheben, ist die spätere Nutzung im Strafverfahren nicht mit einer Zweckänderung verbunden.

Obwohl die Fernwirkungsproblematik damit den allgemeinen Regeln unterliegt, wird man im Zusammenhang mit Geheimdienstinformationen die Annahme einer Fernwirkung weitaus häufiger bejahen müssen als im Bereich der Strafverfolgung.[768] Diese Besonderheit beruht zu einem wesentlichen Teil darauf, dass das Nachrichtendienstrecht mehr als andere Bereiche von speziellen Verwendungsregeln durchzogen wird. Diese beschränken die Verwendung auf den gesetzlich bestimmten Zweck und schließen umgekehrt eine darüber hinausgehende Nutzung umfassend aus. Dieser Ausschluss betrifft sowohl die unmittelbare als auch die mittelbare Beweisnutzung. Eine dem Verwendungsverbot widersprechende Heranziehung mittelbar gewonnener Beweismittel würde nicht nur die Vorgaben des Trennungsgebots, sondern zugleich die in der Verwendungsregel getroffene Entscheidung des Gesetzgebers unterlaufen.[769] Davon unabhängig wird zugunsten

---

[765] Ebenso für die Weitergabe trotz bestehender Löschungspflichten als Unterfall der Verarbeitung i.S.d. § 3 BDSG, vgl. *Rehbein,* S. 210; vgl. insgesamt *Singelnstein,* ZStW 120 (2008), S. 890, ähnlich *Grawe,* S. 284f. Allgemein *Weichert,* S. 218ff.

[766] Vgl. *Dencker,* FS für *Meyer-Goßner*, S. 248f; *Welp,* NStZ 1995, S. 604.

[767] Vgl. *Droste,* Handbuch, S. 227; *Singelnstein,* ZStW 120 (2008), S. 890. Allgemein zur Fernwirkung bei der Zufallsverwendung *Grawe,* S. 274ff.

[768] Vgl. etwa BGHSt 29, 244ff; OLG Köln NJW 1979, S. 1216.

[769] Vgl. *Singelnstein,* ZStW 120 (2008), S. 891.

einer Fernwirkung vereinzelt die Notwendigkeit einer Disziplinierung der Nachrichtendienste angeführt, da dieser im geheim agierenden Nachrichtendienstwesen ein größeres Gewicht zukomme als im grundsätzlich auf Transparenz angelegten Strafverfolgungssektor.[770] Im Anwendungsbereich des G10 wurde die generelle Fernwirkung von Verstößen gegen die Anordnungsvoraussetzungen der §§ 1, 3 G10 zudem höchstrichterlich anerkannt.[771] Im Ergebnis wird einem Verwertungsverbot in Bezug auf nachrichtendienstliche Erkenntnisse öfter als sonst eine Fernwirkung zugesprochen.[772]

d) Aktuelle Kritik an den Verwertungsregeln

Die Kritik an den konkreten Verwertungsregeln fokussiert sich vor allem auf die mit der Einfügung des § 161 II StPO gefundene Regelung. Die Bedenken beziehen sich hierbei unter anderem (1.) auf die Behandlung von Erhebungsmaßnahmen, die nicht in der StPO geregelt sind, (2.) auf die Verwendbarkeit von nur im Einzelfall eingriffsintensiven Maßnahmen, (3.) auf die Handhabung von Erkenntnissen, die lediglich bei Gelegenheit anfallen, (4.) auf Unsicherheiten bei Bestehen einer Sperrerklärung nach § 96 StPO sowie (5.) auf die unbegrenzte Nutzung als Spurenansatz.

aa) Fehlen strafprozessualer Ermächtigungsgrundlagen

Der erste Kritikpunkt bezieht sich auf Sachverhaltskonstellationen, in denen eine vergleichbare strafprozessuale Ermächtigungsgrundlage fehlt.[773] Eine solche Konstellation ist beispielsweise bei Erkenntnissen aus einer optischen Wohnraumüberwachung oder einer strategischen Fernmeldeüberwachung denkbar. In diesem Fall scheidet die direkte Anwendung des hypothetischen Ersatzeingriffs nach § 161 II StPO mangels prüfbarer Parallelermächtigung in der StPO aus. Da diese Maßnahmen eine erhebliche Eingriffsintensität aufweisen, ist auch keine ergänzende Heranziehung des allgemein formulierten § 161 I StPO möglich.[774] Ebensowenig kommt eine analoge Anwendung des § 161 II StPO in Betracht, da es an der Planwidrigkeit der Lücke mangelt. Das Institut des hypothetischen Ersatzeingriffs

---

[770] Vgl. zu diesem Argument *Heine,* HRRS 2009, S. 547 m.w.N.

[771] Vgl. BGHSt 20, 244, 249ff; *Roggan,* G10, § 3 Rn. 12.

[772] Vgl. *Rehbein,* S. 284. Für eine generelle Fernwirkung *Singelnstein,* ZStW 120 (2008), S. 891.

[773] Aufgrund der Annäherung der verschiedenen Ermittlungsbefugnisse ist diese Konstellation jedoch relativ selten.

[774] Eine Heranziehung des § 161 I StPO scheidet aus, weil dieser der Anforderung einer hinreichenden Bestimmtheit nicht genügt. Die Vorschrift ist daher nur auf Bagatellinformationen oder solche von geringer Grundrechtsrelevanz anwendbar.

wurde vom Gesetzgeber eingefügt, um eine Umgehung der strikten Vorgaben der Strafprozessordnung zu verhindern.[775] Verzichtet der Gesetzgeber bereits auf die Einfügung einer vergleichbaren Erhebungsbefugnis in die Strafprozessordnung, bringt er dadurch zum Ausdruck, dass die Strafverfolgungsbehörden gerade keinen Zugriff auf derart erhobene Daten haben sollen. Die mit den exklusiven Erhebungsbefugnissen verfolgten öffentlichen Interessen sind vielmehr auf nachrichtendienstliche Zwecke begrenzt. Nachrichtendienstliche Erkenntnisse, für die keine vergleichbare Befugnis in der Strafprozessordnung vorhanden ist, unterliegen daher im Umkehrschluss einem Beweisverwendungsverbot.[776]

bb) Eingriffsintensität im Einzelfall

Der zweite Kritikpunkt betrifft die Nutzung von Daten, die nur im Einzelfall eine besondere Eingriffsintensität aufweisen. Eine derartige Sonderbelastung kann aus dem Datenumfang oder der Betroffenheit Dritter resultieren.[777] In diesem Fall scheidet eine direkte Subsumtion unter die Voraussetzungen des § 161 II StPO aus, da der Wortlaut der Norm nur Erhebungsmaßnahmen mit generell besonderer Intensität abdeckt.[778] Auch die Vorschrift des § 161 I StPO kann nicht herangezogen werden, da diese eine Zweckänderung lediglich für Bagatellinformationen oder Maßnahmen mit geringer Grundrechtsrelevanz rechtfertigen kann. Anders als im vorgenannten Fall wird eine analoge Heranziehung des § 161 II StPO hier für möglich gehalten.[779] Da der hypothetische Ersatzeingriff die Zweckumwidmung von Daten aus generell eingriffsintensiven Maßnahmen gestattet, müsse dies erst recht für Daten gelten, die nur im Einzelfall eine derartige Intensität erreichen. Diese Konstellation hätte der Gesetzgeber bei Einfügung des § 161 II StPO nicht bedacht, sodass eine analoge Anwendung zur Schließung der planwidrigen Regelungslücke mit Blick auf die vergleichbare Interessenslage sinnvoll erscheine.

cc) Informationsgewinnung bei Gelegenheit

Ein dritter Kritikpunkt betrifft Unklarheiten bei der Verwendung von Erkenntnissen, die nur bei Gelegenheit einer eingriffsintensiven Maßnahme anfallen. Da in diesem Fall die Erkenntnisse nicht auf der spezifischen Eingriffsintensität der

---

[775] Vgl. BT-Drs. 16/5846, S. 64.

[776] Vgl. KK-*Griesbaum,* § 161 Rn. 35; Krekeler/Löffelmann-*Walther,* § 161 Rn. 23.

[777] Vgl. *Singelnstein,* ZStW 120 (2008), S. 876. Allgemein zur Drittbetroffenheit *Rogall,* ZStW 103 (1991), S. 942f.

[778] So *Singelnstein,* ZStW 120 (2008), S. 876.

[779] Vgl. *Singelnstein,* ZStW 120 (2008), S. 876.

geheimdienstlichen Erhebungsmaßnahme beruhen, wollen manche Autoren von einer Anwendung des § 161 II StPO absehen.[780] Der Anwendungsbereich des hypothetischen Ersatzeingriffs sei nicht eröffnet, da die Erkenntnisse gerade nicht i.S.d. § 161 II StPO „auf Grund" der Maßnahme erzielt wurden. Als Beispiel wird der im Zusammenhang mit der nachrichtendienstlichen Beobachtung zur Kenntnis gelangte Autodiebstahl angeführt.[781] Ereignet sich dieser in der Öffentlichkeit, beruht die Kenntnisnahme nicht auf der spezifischen Heimlichkeit der Maßnahme. Die Informationen wären auch ohne langfristig angelegte Beobachtung im normalen Ermittlungsalltag angefallen, sodass sie über § 161 I StPO Eingang in ein Strafverfahren finden sollen. Diese Ansicht lässt jedoch den geheimdienstlichen Erhebungskontext und die Eigenarten geheimdienstlicher Ermittlungen unberücksichtigt. Der Vorfeldbezug der nachrichtendienstlichen Beobachtungsmaßnahmen bleibt völlig außer Betracht. Im Übrigen würde die Einführung von Erkenntnissen bei einfacher Kriminalität bereits an den Übermittlungsvorschriften scheitern.

dd) Unsicherheiten bei Sperrerklärungen

Eine vierte Schwierigkeit entsteht beim Vorliegen einer Sperrerklärung nach § 96 StPO.[782] Diese setzt der Pflicht zur Aktenvorlage staatlicher Behörden gegenüber den Strafverfolgungsbehörden Grenzen.[783] Durch die Zurückhaltung wichtiger Details ist das Gericht bei Anwendung des § 161 II StPO nicht in der Lage, den konkreten Sachverhalt im Sinne des hypothetischen Ersatzeingriffs nachzustellen. In der Konsequenz kann der Richter nicht überprüfen, ob die Strafverfolgungsbehörden zur Erhebung des fraglichen Beweismittels in der Lage gewesen wären. Diese Schwierigkeiten sind allerdings mit Blick auf den Charakter der Verwendungsregel behebbar. In diesem Sinne wird die Vorschrift § 161 II StPO als eine Verbotsnorm mit eng auszulegendem Erlaubnisvorbehalt verstanden.[784] Zweifel führen dementsprechend zur Unverwertbarkeit der zu überprüfenden Information. Dieses Verständnis trägt dem Grundsatz Rechnung, dass sich Unsicherheiten nicht zulasten des Angeklagten auswirken dürfen. Ist dementsprechend nach der Heranziehung aller Erkenntnisse unklar, ob die Voraussetzungen des hypothetischen Ersatzeingriffs vorliegen, scheidet eine Verwertung aus.

---

[780] So *Allgayer/Klein,* wistra 2010, S. 131, bzgl. der parallelen Verwendungsregel des § 477 II 2 StPO.

[781] Vgl. *Allgayer/Klein,* wistra 2010, S. 131.

[782] Vgl. *Grawe,* S. 177 Fn. 500.

[783] Nähere Einzelheiten werden im Rahmen der Geheimhaltungsproblematik dargestellt.

[784] So *Eisenberg,* Rn. 358; *Knieriem,* StV 2008, S. 601.

ee) Nutzung als Spurenansatz

Ein fünfter Kritikpunkt betrifft die unbeschränkte Heranziehung nachrichtendienstlicher Erkenntnisse als Spurenansatz.[785] Nach dem ausdrücklichen Willen des Gesetzgebers wird durch die Vorschrift des § 161 II StPO ausschließlich die Verwendung zu Beweiszwecken limitiert.[786] Die Nutzung zu weiteren Ermittlungen unterliegt demgegenüber keinen Verwendungsbeschränkungen. Da die weiteren Erkenntnisse folglich auf der Grundlage der StPO erhoben werden, ist die Verwertung weder mit einer Zweckänderung noch einem Grundrechtseingriff verbunden.[787] Diese unreflektierte Beweisverwertung übersieht jedoch, dass die Nutzung als Spurenansatz ebenfalls eine Zweckänderung darstellt und damit einer hinreichend bestimmten Ermächtigungsgrundlage bedarf.[788] Ob die beweisrechtlichen Folgen unmittelbar oder mittelbar zum Tragen kommen, ist insofern irrelevant.[789] Obwohl eine derartige Ermächtigung fehlt, geht der Gesetzgeber von einer vollumfänglichen Nutzbarkeit nachrichtendienstlicher Erkenntnisse als Spurenansatz aus und gestattet damit die mittelbare Umgehung der in § 161 II StPO normierten Voraussetzungen. Denkt man den vom Gesetzgeber vertretenen Ansatz zu Ende, müsste bereits eine von vorneherein auf den Ermittlungsansatz zielende Informationserhebung ohne Beschränkungen zulässig sein.[790] Derartige Abstufungen sind in der Strafprozessordnung nicht vorgesehen. Vielmehr gelten üblicherweise die gleichen Erhebungsvoraussetzungen unabhängig davon, ob die Maßnahme der Erlangung von Beweismitteln oder von Ermittlungsansätzen dient. Im Widerspruch zur gesetzlichen Lösung wäre es daher konsequent die Verwendung als Spurenansatz den gleichen Regeln wie der unmittelbaren Verwertung zu unterwerfen. Da eine verfassungskonforme Auslegung am eindeutigen Wortlaut des Gesetzes scheitert, wäre eine Klarstellung durch den Gesetzgeber wünschenswert. Eine derartige Gesetzesanpassung müsste die besonderen Herausforderungen dieser Problematik berücksichtigen. Da für die Nutzung als Spurenansatz bereits die bloße Kenntnisnahme genügt, müsste die Regelung zusätzliche Kontrollmechanismen vorsehen.[791]

---

[785] Vgl. hierzu *Hefendehl,* GA 2011, S. 224f; Radtke/Hohmann-*Kretschmer,* § 161 Rn. 14f; *Rogall,* JZ 2008, S. 828. Kritisch zur „Spurenansatz-These" bereits *Wolter,* ZStW 107 (1995), S. 817, 819.

[786] So ausdrücklich BT-Drs. 16/5846, S. 6; vgl. zudem BGH NJW 1978, S. 1390; BGH NStZ 1998, S. 426f, sowie BVerfG, 2 BvR 866/05 vom 29.6.2005, NJW 2005, S. 2766. Vgl. zu dieser Problematik *Eisenberg,* Rn. 2502; *Lohberger,* FS für Hanack, S. 260ff.

[787] Vgl. *Rehbein,* S. 142f; *Rogall,* ZStW 1996, S. 929. Die entsprechende Verwertungsbefugnis ist in der strafprozessualen Erhebungsbefugnis mit enthalten, vgl. *Rogall,* ZStW 103 (1991), S. 952.

[788] Vgl. Radtke/Hohmann-*Kretschmer,* § 161 Rn. 15; *Singelnstein,* ZStW 120 (2008), S. 885.

[789] Vgl. *Singelnstein,* ZStW 120 (2008), S. 886.

[790] Vgl. zu dieser Gegenprobe *Singelnstein,* ZStW 120 (2008), S. 886.

[791] Mit Vorschlägen *Hefendehl,* GA 2011, S. 230.

e) Zwischenergebnis zu Verwertungsregeln

Die Nutzung von Geheimdienstinformationen zu Beweiszwecken richtet sich im Wesentlichen nach den in § 161 II StPO aufgestellten Vorgaben. Danach dürfen personenbezogene Daten aus generell eingriffsintensiven Maßnahmen nur bei Vorliegen einer Einwilligung oder einer Bejahung der Voraussetzungen des hypothetischen Ersatzeingriffs zu Beweiszwecken verwendet werden. Im letzteren Fall prüft der Richter, ob die Erkenntnisse hypothetisch nach den Voraussetzungen der Strafprozessordnung hätten erhoben werden können. Diese Anforderungen werden durch spezialgesetzliche Verwendungsbeschränkungen und die allgemeinen Verwertungsregeln ergänzt. Der Anwendungsbereich des § 161 II StPO selbst ist auf generell eingriffsintensive Maßnahmen limitiert. Nicht-personenbezogene Daten oder Daten aus nicht eingriffsintensiven Erhebungsmaßnahmen dürfen über § 161 I StPO in das Strafverfahren eingeführt werden. Die Nutzung geheimdienstlicher Erkenntnisse als Spurenansatz ist demgegenüber in vollem Umfang möglich. Fehler im geheimdienstlichen Erhebungs- und Übermittlungsprozess werden grundsätzlich nach den allgemeinen Verwertungsregeln berücksichtigt. Aufgrund der zahlreichen nachrichtendienstlichen Verwendungsregeln sind diese jedoch häufiger als sonst mit einem Verwertungsverbot oder einer Fernwirkung verbunden. Rechtswidrige beziehungsweise rechtswidrig erlangte Geheimdienstinformationen dürfen damit im Grundsatz nicht zum Nachteil einer Person verwertet werden. Ausnahmen sind indes bei einer Verwertung zugunsten des Angeklagten denkbar. Insgesamt sind die Regelungen mit zahlreichen Unsicherheiten behaftet. Die vorgebrachten Kritikpunkte verdeutlichen zudem die verbleibenden Risiken und Defizite, die mit einer Einbeziehung des Geheimdienstsektors verbunden sind. Diese befassen sich vor allem mit Aspekten des Trennungsgebots und des Grundrechtsschutzes.

IV. Auswirkungen staatlicher Geheimhaltung

Der zweite zentrale Themenkreis dieser Arbeit ist die staatlich veranlasste Geheimhaltung. Danach können nationale Sicherheitsinteressen trotz eines begründeten Strafverfolgungsbedürfnisses einer Offenlegung geheimdienstlicher Erkenntnisse entgegenstehen. Die bei einer staatlichen Geheimhaltung bestehenden Interessens- und Rechtskonflikte werden zunächst im Überblick dargestellt (A.). Im Anschluss daran werden die rechtlichen Möglichkeiten und Grundlagen einer Geheimhaltung anhand eines Stufenmodells herausgearbeitet (B.). Zum Abschluss werden die verschiedenen Geheimhaltungs- und Kompensationsmodelle einer kritischen Würdigung unterzogen (C.).

A. Interessens- und Rechtskonflikte bei staatlicher Geheimhaltung

Staatliche Geheimhaltungsinteressen stehen im prinzipiellen Widerspruch zu den Grundsätzen eines öffentlichen Strafverfahrens. Dennoch existieren Sachverhalte, die einen vollständigen oder teilweisen Geheimnisschutz notwendig erscheinen lassen. Da sich der nachrichtendienstliche Beobachtungsauftrag auf besonders sensible oder sicherheitsrelevante Beobachtungsfelder erstreckt, ist die Exekutive dort häufiger als in anderen Sicherheitsbereichen auf eine Geheimhaltung angewiesen. Sollen nun Geheimdienstinformationen als Beweismittel eingeführt werden, steht der Staat vor dem Dilemma, dass er gleichzeitig den Offenlegungspflichten und den Geheimhaltungsinteressen gerecht werden soll. Die Brisanz dieses Konflikts wird bei einer Gegenüberstellung der unterschiedlichen, widerstreitenden Interessen besonders deutlich. Aus diesem Grund werden nachfolgend die im deutschen Kontext bestehenden Geheimhaltungsinteressen des Staates einerseits und die Offenlegungspflichten beziehungsweise Teilhaberechte des Angeklagten andererseits herausgearbeitet.

1. Geheimhaltungsinteressen des Staates

Die Geheimhaltungsinteressen des Staates können im Zusammenhang mit der nachrichtendienstlichen Informationsgewinnung auf unterschiedliche Erwägungen gestützt werden. Zentraler Anknüpfungspunkt für eine staatliche Geheimhaltung ist der sogenannte Quellenschutz.[792] Dieser betrifft sowohl den Schutz aktueller als auch die Gewinnung neuer Informationsquellen. Beides wird durch eine Nutzung nachrichtendienstlicher Erkenntnisse im Strafverfahren in Mitleidenschaft gezogen. In Bezug auf aktuelle Informationsquellen kann sie zur Offenlegung einer langwierigen und kostenintensiven Legendierung führen, wodurch die Quelle strategisch nutzlos wird.[793] Darüber hinaus kann eine zu offensive Offenlegungstaktik das Vertrauen anderer Informanten oder ausländischer Dienste beschädigen.[794] Ein solcher Vertrauensverlust kann die Rekrutierung neuer Informationsquellen beziehungsweise die Zusammenarbeit mit ausländischen Diensten erheblich erschweren und sich massiv auf die Handlungsfähigkeit der Dienste auswirken.[795] Die Gewährleistung einer gewissen Anonymität ist für die Dienste damit bereits aus Effektivitätsgründen von oberster Priorität. Für den betroffenen Informanten selbst ist der Quel-

---

[792] Zur Notwendigkeit des Geheimnisschutzes vgl. BbgVerfG, NVwZ-RR 2005, S. 299, 301; *Schäfer/Wache/Meiborg*, Rn. 351.

[793] Vgl. *P.-A. Albrecht,* StV 2001, S. 106f; *Droste,* Nachrichtendienste, S. 115; *Droste,* Handbuch, S. 280f. Man spricht vom „Verbrennen" der Quelle.

[794] Vgl. *Rebmann,* NStZ 1982, S. 316.

[795] So *Ferse,* KritV 1994, S. 260. Insbesondere V-Leute begeben sich oftmals in Lebensgefahr.

lenschutz von erheblicher persönlicher Bedeutung, wenn Repressalien oder sonstige Racheakte aus der vormals ausgespähten Szene drohen. Trotz eventuell bestehender Strafverfolgungsinteressen obliegen der Exekutive gewisse Fürsorge- und Schutzpflichten, die eine Geheimhaltung rechtfertigen können.[796] Dieser Geheimnisschutz kann im Zweifel dem Interesse an einer Strafverfolgung vorgehen.[797] Schließlich können Geheimhaltungsinteressen aus der Angst vor der Ausforschung geheimhaltungsbedürftiger Bereiche resultieren. Die offengelegten Informationen geben oftmals über den konkreten Einzelfall hinaus Aufschluss über Methoden, Arbeitsweisen und Interessen der Geheimdienste. Eine solche Transparenz kann die Effektivität der Dienste nachteilig beeinflussen, sodass die exekutiven Entscheidungsträger üblicherweise auf eine Geheimhaltung hinwirken werden.

2. Offenlegungspflichten und Teilhaberechte

Die im Strafprozess geltenden Verfahrensgrundsätze und Teilhaberechte stehen oft in Konflikt mit einer staatlich veranlassten Geheimhaltung. Grundlegendes Ziel jedes Strafverfahrens ist die Erforschung der materiellen Wahrheit.[798] Diesem Zweck dienen verschiedene Prinzipien der Strafprozessordnung, die durch eine staatlich veranlasste Zurückhaltung relevanter Informationen beeinträchtigt werden können. Hiervon sind unter anderem der Grundsatz der Unmittelbarkeit, der Öffentlichkeit, der Mündlichkeit sowie die richterliche Aufklärungspflicht und Unabhängigkeit betroffen. Bei einer staatlich verkürzten Beweisgrundlage werden diese Prinzipien zum Teil erheblich eingeschränkt. Die nach dem Unmittelbarkeitsgrundsatz gewährleistete Beweisaufnahme des sachnächsten und direktesten Beweismittels ist nicht möglich, wenn dieses der Geheimhaltung unterliegt.[799] Ebenfalls eingeschränkt wird die durch den Öffentlichkeitsgrundsatz gestattete Kenntnis von den Vorgängen der Hauptverhandlung. Die staatliche Abschottung relativiert die zu gewährleistende Kontrolle des Staates, die Unabhängigkeit der Gerichte und das Vertrauen der Allgemeinheit in die Justiz.[800] Zudem kann der Richter die Beweisaufnahme nicht auf sämtliche und bestmögliche Beweismittel erstrecken, obwohl er hierzu nach der richterlichen Aufklärungspflicht verpflichtet wäre.[801] Eine Geheimhaltung verfahrensrelevanter Umstände gerät mit den Postulaten des Strafverfahrensrechts damit zwangsläufig in Konflikt.

---

[796] Die Schutzpflicht resultiert aus Art. 2 II 1, 1 I 2 GG; vgl. *Droste,* Handbuch, S. 281.

[797] Vgl. *Droste,* Handbuch, S. 281.

[798] BVerfG NStZ 1987, S. 419; BVerfGE 57, 250, 275.

[799] Vgl. § 250 StPO. Damit werden die materielle und formelle Komponente des Unmittelbarkeitsgrundsatzes angesprochen, vgl. *Joecks*, Einl. 164.

[800] Vgl. Graf-*Allgayer,* § 169 GVG Rn. 3; KK-*Diemer,* § 169 GVG Rn. 2. Der Öffentlichkeitsgrundsatz dient dem Informationsinteresse, ohne dem Einzelnen ein subjektives Recht einzuräumen.

[801] Vgl. § 244 II StPO sowie *Eisenberg,* Rn. 1031.

Daneben kann eine Geheimhaltung die Verteidigungsinteressen des Beschuldigten beziehungsweise Angeklagten belasten. Denkbar sind nachteilige Auswirkungen auf den Anspruch auf rechtliches Gehör, das Fragerecht sowie den Grundsatz eines fairen Verfahrens.[802] Der Anspruch auf rechtliches Gehör aus Art. 103 I GG gewährt dem Angeklagten Informations-, Äußerungs- und Beteiligungsrechte, durch die er unter anderem auf eine Offenlegung beziehungsweise Heranziehung sachnäherer Beweismittel drängen kann.[803] Diese Rechte werden erheblich beschnitten, wenn das sachnächste Beweismittel gerade der Geheimhaltung unterliegt. Dies gilt in gleicher Weise für den Schutz eines als Belastungszeuge auftretenden Informanten, dessen Glaubwürdigkeit der Angeklagte bei einer Geheimhaltung nicht durch direkte Fragen testen kann.[804] Schließlich können je nach Umfang der Geheimhaltung die durch den Grundsatz des fairen Verfahrens verbürgten Mindeststandards an aktiven Teilhabe- und Einflussmöglichkeiten beeinträchtigt werden.[805] Seine Verteidigungsinteressen kann der Angeklagte effektiv nur bei Kenntnis aller entscheidungserheblichen Tatsachen wahrnehmen.[806] Die Strafprozessordnung versteht den Angeklagten insofern nicht nur als Verfahrensobjekt, sondern nimmt ihn als ein das Verfahren aktiv beeinflussendes Verfahrenssubjekt ernst.[807] Eine staatliche veranlasste Geheimhaltung steht hierzu im Widerspruch. Im Ergebnis gebieten damit sowohl das strafprozessuale Interesse an der Wahrheitsfindung als auch die Verteidigungs- und Informationsinteressen des Angeklagten eine restriktive Handhabung der Geheimhaltungsregeln.[808]

B. Rechtliche Möglichkeiten der Geheimhaltung

Sowohl der Gesetzgeber als auch die Rechtsprechung versuchen den Konflikt zwischen Geheimhaltungs- und Offenlegungsinteressen durch verschiedene Mechanismen und Ersatzstrategien zu lösen. In diesem Sinne existieren in der Straf-

---

802 Insgesamt zu den Beteiligungsrechten *Roxin/Schünemann,* § 18 Rn. 3ff.

803 Vgl. BVerfG NStZ-RR 2008, S. 16f; BVerfG NJW 2004, S. 2443, NJW 1980, S. 2698; BVerfG NJW 1981, S. 1719, 1721; Epping/Hillgruber-*Radtke/Hagemeier,* Art. 103 Rn. 1.

804 Vgl. *Eisenberg,* Rn. 792; *Pfeiffer* StPO, § 240 Rn. 1; KK-*Schneider,* § 240 Rn. 1.

805 Vgl. BVerfG NJW 1981, S. 1719, 1722; *Droste,* Handbuch, S. 589; *Zöller,* StraFo 2008, S. 17. Das Fragerecht leitet sich aus dem Rechtsstaatsprinzip i.V.m. dem allgemeinen Freiheitsrecht sowie der freiheitssichernden Funktion der Grundrechte ab, vgl. Art. 20 III GG i.V.m. Art. 2 I GG; BVerfG NStZ 2006, S. 46f; BVerfG NJW 1981, S. 1719. Ähnliche Verbürgungen finden sich auch in der Menschenrechtskonvention in Art. 6 I, III EMRK.

806 So Epping/Hillgruber-*Radtke/Hagemeier,* Art. 103 Rn. 8f.

807 Vgl. BVerfG NJW 1983, S. 1599; BVerfG NJW 1978, S. 151, sowie *Schlegel,* HRRS 2004, S. 411. Dies war in der Reichstrafprozessordnung vom 1.2.1877 noch anders.

808 Vgl. *Wolff,* JZ 2010, S. 176.

prozessordnung, den Nachrichtendienstgesetzen und der Judikatur verschiedene Geheimhaltungs- und Beweisregeln, die dazu beitragen sollen, den genannten Interessens- und Rechtskonflikten gerecht zu werden. Die rechtlichen Möglichkeiten dieser Geheimhaltungsregeln werden aus Gründen der Verständlichkeit anhand schlagwortartig bezeichneter „Strategien" kategorisiert: erstens die vollständige Abschottung, zweitens eine auf den Richter begrenzte Offenlegung, drittens die ergänzende Beiziehung des Verteidigers unter Ausschluss seines Mandanten, viertens den Ausschluss der Geschworenen und fünftens den Ausschluss der Öffentlichkeit. Im Folgenden werden diese Geheimhaltungsstrategien mit ihren für eine Geheimhaltung erforderlichen Voraussetzungen sowie den Auswirkungen auf das Strafverfahren dargestellt. Falls vorhanden, wird auf bestehende Kompensationsmechanismen eingegangen.

1. Strategie der vollständigen Abschottung

Nach der ersten Geheimhaltungsstrategie werden die strafrechtlich relevanten Informationen allen Verfahrensbeteiligten gegenüber geheim gehalten. Eine solche Geheimhaltung ist sowohl unter den Voraussetzungen des § 23 BVerfSchG als auch des § 96 StPO denkbar.

a) Vor der Hauptverhandlung

Im Vorfeld einer Hauptverhandlung kann eine vollständige Geheimhaltung auf einer Geheimhaltungsentscheidung der Nachrichtendienste, der Staatsanwaltschaft oder der Exekutive beruhen.

aa) Geheimhaltungsentscheidung der Nachrichtendienste

Eine vollständige Geheimhaltung kann auf Basis der Nachrichtendienstgesetze erfolgen. In diesem Fall handelt es sich um eine rein interne Entscheidung, der keine Verwaltungsaktqualität zukommt.[809]

(1) Voraussetzungen der Geheimhaltung

Die für eine Geheimhaltung erforderlichen Voraussetzungen finden sich in § 23 BVerfSchG gegebenenfalls i.V.m. den §§ 12 MADG, 10 BNDG. Die Geheimhaltungsentscheidung wird bereits im Vorfeld einer Übermittlung getroffen,

[809] Es fehlt insofern am Regelungscharakter und der unmittelbaren Rechtswirkung nach außen i.S.d. § 35 VwVfG.

sodass die nachrichtendienstlichen Erkenntnisse den Geheimdienstsektor erst gar nicht verlassen. Für den Beschuldigten ist diese Konstellation vor allem bei einer Geheimhaltung entlastenden Beweismaterials von Interesse.

Nach § 23 BVerfSchG unterbleibt eine Übermittlung an Stellen außerhalb des Geheimdienstsektors, wenn die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an einer Übermittlung überwiegen (Nr. 1), überwiegende Sicherheitsinteressen ein Unterlassen der Übermittlung erfordern (Nr. 2) oder besondere gesetzliche Übermittlungsregelungen entgegenstehen (Nr. 3).[810] Das Eingreifen der Übermittlungssperre nach § 23 Nr. 1 BVerfSchG bestimmt sich anhand einer Abwägung, deren Ausgang sich außer nach der Qualität und Relevanz der Information nach der Sensibilität und der Intensität des Eingriffs in das Persönlichkeitsrecht des Betroffenen richtet.[811] Eine Zurückhaltung wird bei überwiegenden Persönlichkeitsinteressen sowie bei eher unbedeutenden Erkenntnissen gestattet, die unter Einsatz besonders eingriffsintensiver Maßnahmen erlangt wurden.

Die Übermittlungssperre nach § 23 Nr. 2 BVerfSchG erfordert ebenfalls eine Abwägung. Diese erfolgt zwischen den Sicherheitsinteressen einerseits und dem öffentlichen Interesse an der Verfolgung von Staatsschutzdelikten andererseits. Die Sicherheitsinteressen können sich etwa aus Gründen des Quellen- und Methodenschutzes ergeben.[812] Um eine Gefährdung des Beobachtungsauftrags der Dienste zu verhindern, werden die Entscheidungsträger im Geheimdienstsektor üblicherweise von einem Überwiegen der nachrichtendienstlichen Geheimhaltungsinteressen ausgehen. Umgekehrt können besonders hochrangige Rechtsgüter oder schwerwiegende Straftaten die Abwägung zugunsten einer Übermittlungspflicht beeinflussen.[813]

Die letzte Variante nach § 23 Nr. 3 BVerfSchG erfasst die Unzulässigkeit einer Übermittlung aufgrund einer entgegenstehenden Gesetzeslage. Diese kann durch Vorschriften zum Sozial- und Steuergeheimnis oder Übermittlungsverbote der Abgabenordnung erzeugt werden.[814] Durch die Schaffung der Übermittlungssperre des § 23 BVerfSchG hat der Gesetzgeber die Entscheidung über den Zugang zu nachrichtendienstlichen Erkenntnissen primär den Nachrichtendiensten überlassen.[815] Sämtliche Übermittlungsvorgänge stehen unter dem Vorbehalt des § 23 BVerf

---

[810] Vgl. *Baumann,* FS für Posser, S. 307.

[811] Vgl. BT-Drs. 11/4306, S. 64; *Droste,* Handbuch, S. 553.

[812] Vgl. *Droste,* Handbuch, S. 554.

[813] Vgl. *Droste,* Handbuch, S. 554. Vgl. zum Verhältnis zu § 138 StGB *Rehbein,* S. 120, 121.

[814] Vgl. hierzu *Droste,* Handbuch, S. 555; SK-StPO-*Wohlers,* § 96 Rn. 3.

[815] So *Griesbaum,* FS für Nehm, S. 134. Das Übermittlungsverbot gilt damit nicht für Übermittlungen zwischen den verschiedenen Verfassungsschutzbehörden, vgl. *Droste,* Handbuch, S. 553. Hierfür gelten die §§ 5ff BVerfSchG.

SchG.[816] Werden dessen Voraussetzungen bejaht, können die nachrichtendienstlichen Erkenntnisse bereits im Vorfeld eines Ermittlungsverfahrens gegenüber allen Beteiligten geheim gehalten werden.

(2) Auswirkungen auf das Strafverfahren

Die Geheimhaltungsentscheidung der Nachrichtendienste wirkt sich bei der Zurückhaltung belastender Erkenntnisse für den Betroffenen zumindest nicht negativ aus, da der Staat eigenständig auf seinen Strafanspruch verzichtet. Sind von der Übermittlungssperre jedoch entlastende Informationen betroffen, kann diese Geheimhaltungsstrategie negative Auswirkungen haben. Nachteile ergeben sich insbesondere dann, wenn bereits aufgrund anderer Hinweise ein Strafverfahren eröffnet wurde und dem Betroffenen relevante Beweismittel vorenthalten werden. Da im letzten Fall die Informationen das nachrichtendienstliche Innenverhältnis nicht verlassen, können weder der Beschuldigte noch das Gericht gegen die Übermittlungssperre vorgehen. Der Richter kann seiner Entscheidungsfindung folglich nur die ihm zur Verfügung stehenden Beweismittel zugrunde legen. Mangels Kenntnis kann er die staatlich bedingte Geheimhaltung nicht zugunsten des Angeklagten berücksichtigen. Bestehen allerdings Anhaltspunkte für eine Beteiligung der Nachrichtendienste, muss das Gericht diesen aufgrund seiner Aufklärungspflicht nachgehen. Insgesamt wird der Betroffene durch die Übermittlungssperre damit nicht wesentlich schlechter gestellt, als er ohne die Beteiligung der Dienste stände. Den Diensten ist insofern eine bewusst irreführende und selektive Übermittlung belastendender Beweise untersagt. Zudem sind die Strafverfolgungsorgane ihrerseits von Amts wegen zur Erforschung des Sachverhalts unter Berücksichtigung entlastender Aspekte verpflichtet. Kann der Richter selbst auf dieser Grundlage keine persönliche Gewissheit gewinnen, muss er im Zweifel zugunsten des Angeklagten entscheiden.

bb) Geheimhaltungsentscheidung der Staatsanwaltschaft

(1) Voraussetzungen der Geheimhaltung

Eine Geheimhaltung auf Initiative der Staatsanwaltschaft ist möglich, wenn diese (vorübergehend) auf die Aufnahme sensibler Informationen in die Verfahrensakten verzichtet.[817] Ein Verzicht kann etwa auf einer Vertraulichkeitsbitte der Nachrichtendienste und der damit korrespondierenden Vertraulichkeitszusage der Staatsanwaltschaft basieren. Ein solches Vorgehen kommt beispielsweise aus Quellen-

816 So *Rehbein,* S. 121.

817 So kann etwa nach § 68 IV 3, 4 StPO auf die Aufnahme von Angaben zur Person und deren Wohnort verzichtet werden, vgl. *Zacharias,* S. 210, 285.

schutzgründen in Betracht.[818] Die vertraulichen Informationen werden von der Staatsanwaltschaft in einer separaten Sonderakte geführt, sodass sich die Informationserhebung zunächst allein zwischen den Nachrichtendiensten und den Strafverfolgungsbehörden vollzieht.[819] Aber selbst wenn die Informationen Eingang in die Akten finden, kann die Staatsanwaltschaft die Akteneinsicht nach § 147 II i.V.m. V 1 StPO bis zur Anbringung des Abschlussvermerks i.S.d. § 169a StPO verweigern. Voraussetzung ist eine andernfalls drohende Gefährdung des Untersuchungszwecks, deren Vorliegen die Staatsanwaltschaft nach einer Abwägung feststellt.[820] In dieser Abwägung werden die Verteidigungs- und Aufklärungsinteressen unter Berücksichtigung der besonderen Bedeutung des Ermittlungsverfahrens für die Sachverhaltsaufklärung einander gegenübergestellt.[821] Da nachrichtendienstliche Erkenntnisse oftmals gerade den Bereich der sensiblen Strukturaufklärung betreffen, ist ein solcher Aufschub des Akteneinsichtsrechts zur Sicherung des Untersuchungszwecks durchaus denkbar.

In Bezug auf eine Geheimhaltungsentscheidung der Staatsanwaltschaft werden jedoch erhebliche Bedenken geäußert. Insbesondere die auf eine Vertraulichkeitsbitte gestützte Nichtaufnahme von Erkenntnissen in die Verfahrensakten ist als Geheimhaltungsinstrument vom Gesetzgeber nicht vorgesehen. Eine dennoch erfolgende Zurückhaltung der Erkenntnisse kollidiert mit den Vorgaben der §§ 163 II 1, 199 II 2 StPO sowie dem Gebot der Aktenvollständigkeit und -wahrheit.[822] Entgegen der Verzichtserklärung müssen die Erkenntnisse mit Übersendung an die Staatsanwaltschaft vielmehr Bestandteile der Akten i.S.d. § 147 I StPO werden.[823] Diese Verfahrensakten sind dem Gericht vorzulegen und müssen sämtliche für die Schuld- und Rechtsfolgen relevanten Umstände dokumentieren.[824]

(2) Auswirkungen auf das Strafverfahren

Die Auswirkungen einer Vertraulichkeitszusage auf das Strafverfahren sind gering, da das Gericht nicht an das Versprechen der Staatsanwaltschaft gebunden

---

[818] Vgl. hierzu Anlage D der RiStBV, welche eine gemeinsame Verwaltungsvorschrift des Justizministeriums und des Innenministeriums zur Inanspruchnahme von Informanten und zum Einsatz von Vertrauenspersonen und Verdeckten Ermittlern im Rahmen der Strafverfolgung darstellt. Zudem dürfen nach RiStBV Nr. 213 Abs. 1 geheim zu haltende Tatsachen in den Sachakten nur insoweit schriftlich festgehalten werden, als dies für das Verfahren unerlässlich ist. Abgedruckt bei *Meyer-Goßner,* Anh. 12 RiStBV.

[819] Letztlich verpflichten sich die Strafverfolgungsbehörden damit auch zu einer Geheimhaltung gegenüber dem Gericht, vgl. *Zacharias,* S. 285.

[820] Vgl. SK-StPO-*Wohlers,* § 147 Rn. 94ff.

[821] Vgl. allgemein *Zacharias,* S. 207.

[822] Vgl. Widmaier-*Eschelbach,* § 28 Rn. 22.

[823] Vgl. BGHSt 42, 71f; OLG Hamm NJW 1984, S. 880; *Burhoff,* Rn. 132.

[824] Vgl. *Meyer-Goßner*, § 147 Rn. 14; *Zacharias,* S. 284.

ist.[825] Aus der Perspektive der Geheimdienste ist diese Geheimhaltungsmöglichkeit daher untauglich. Da die staatsanwaltschaftliche Zusage spätestens vor Gericht keine Bindungswirkung mehr entfaltet, kann durch die Absprache kein ausreichender Geheimnisschutz gewährleistet werden.

Kommt es entgegen dieser Regelung aufgrund einer Vertraulichkeitsbitte dennoch zu einem Informationsvorsprung, ist dieser während des Hauptverfahrens auszugleichen. Insofern kann der Richter bei der Beweiswürdigung, wie auch sonst, lediglich die Tatsachen berücksichtigen, die Gegenstand der Hauptverhandlung und somit auch der Verteidigung zugänglich waren.

cc) Geheimhaltungsentscheidung oberster Dienstbehörden

Schließlich können oberste Dienstbehörden durch die Abgabe einer Sperrerklärung eine staatliche Geheimhaltung ermöglichen. Rechtlicher Anknüpfungspunkt ist die Vorschrift des § 96 StPO.[826] Auf der Grundlage einer solchen Sperrerklärung können in direkter oder analoger Anwendung sowohl die Vorlage von Schriftstücken als auch die Erteilung von Auskünften verweigert werden.[827] Hierdurch ist in bestimmten Fällen eine Geheimhaltung gegenüber sämtlichen Verfahrensbeteiligten erzielbar.[828] Die staatliche Geheimhaltung mittels Sperrerklärung bildet im deutschen Recht die wichtigste Geheimhaltungsstrategie für den Bereich der Geheimdienstinformationen. Aufgrund dieser besonderen Relevanz werden die Voraussetzungen und Auswirkungen auf das Strafverfahren an dieser Stelle einer vertieften Untersuchung zugeführt.

---

[825] Vgl. BGHSt 35, 82, 85; *Zacharias,* S. 289. Eine Verlesung von Protokollen kann nicht auf eine Vertraulichkeitszusage gestützt werden, vgl. *J. Meyer,* NStZ 1986, S. 132.

[826] Eine in Geheimhaltungsfragen ergänzende Heranziehung der Regelungen zur Auskunftsverweigerung nach § 54 I StPO i.V.m. den entsprechenden beamtenrechtlichen Vorschriften erübrigt sich, da sich die Vorschrift des § 96 StPO in den Hauptanwendungsfällen der Geheimhaltung als Analogiebasis durchgesetzt hat, vgl. BGHSt 32, 32; BGH NStZ 1984, S. 36, 38; KK-*Senge,* Vor § 48 Rn. 60. Der Unterscheidung bzw. dem Verhältnis beider Vorschriften kommt damit kaum noch eine praktische Bedeutung zu. Vertiefend zur Problematik vgl. *H. Müller,* Geheimhaltung, S. 25ff.

[827] § 96 StPO beschränkt folglich die Herausgabepflicht des § 95 StPO und grenzt die Amtshilfepflicht nach Art. 35 I GG ein.

[828] Das Verhältnis zur Sperrmöglichkeit des § 23 BVerfSchG ist weitgehend ungeklärt. Nach SK-StPO-*Wohlers,* § 96 Rn. 3, können beide Vorschriften eine Zurückhaltung rechtfertigen. Demgegenüber will *Eisenberg,* Rn. 1038, im Strafverfahren allein auf § 96 StPO zurückgreifen. Nach dem vorliegend vertretenen Doppeltürenmodell müssen für eine Übermittlung jedoch stets die die Voraussetzungen der Nachrichtendienstgesetze und damit des § 23 BVerfSchG beachtet werden. § 96 StPO greift dementsprechend, wenn die Informationen den Geheimdienstsektor bereits verlassen haben.

(1) Voraussetzungen der Geheimhaltung

Bei der Sperrerklärung handelt es sich um einen Verwaltungsakt, für dessen Rechtmäßigkeit die formellen und materiellen Voraussetzungen des § 96 StPO erfüllt sein müssen.[829]

(α) Zuständigkeiten

Die Sperrerklärung muss durch die zuständige Stelle verfahrens- und formgerecht abgegeben werden. Die dafür zuständige Stelle ist von der für das Auskunftsverlangen zuständigen Stelle abzugrenzen. In Zuständigkeitsfragen ist damit zwischen der anfragenden Behörde und der sperrenden Behörde zu unterscheiden. Berechtigt zur Anfrage sind, je nach Stand des Verfahrens, die Staatsanwaltschaft oder das Gericht.[830] Für die Abgabe einer Sperrerklärung ist die oberste Dienstbehörde der verwahrenden Stelle und damit in der Regel der oberste Fachminister als Aufsichtsbehörde zuständig.[831] Eine Delegation dieser Befugnis ist nur in wenigen Fällen zulässig.[832] In personeller Hinsicht liegt die Zuständigkeit für die Staatsanwaltschaften beim Justizminister, für die Polizei beim jeweiligen Landesinnenminister und für das Bundeskriminalamt beim Bundesinnenministerium.[833] Im Geheimdienstsektor ist die jeweils oberste Dienstbehörde des ersuchten Nachrichtendienstes zuständig. Bei den Landesämtern für Verfassungsschutz gibt der jeweilige Landesinnenminister, beim BfV der Bundesinnenminister, beim MAD der Bundesverteidigungsminister und beim BND das Bundeskanzleramt die erforderliche Sperrerklärung ab.[834]

(β) Formvorschriften

Weiterhin muss die Sperrerklärung bestimmten Formerfordernissen genügen und den Charakter als Sperrerklärung deutlich erkennen lassen. Nicht ausreichend ist eine bloße Bitte um Vertraulichkeit.[835] Hierzu sollte die Sperrerklärung eine über allgemeine Formulierungen hinausgehende, nachvollziehbare und substantiierte Begründung enthalten, die den jeweiligen Aktenbestandteilen konkret zugeordnet

---

[829] Die zum Teil erörterte Frage, ob § 96 StPO letztlich die Herausgabepflicht des § 95 StPO oder aber die Amtshilfe des Art. 35 I GG regelt, ist für die vorliegende Lösung nicht von Belang und wird daher nicht weiter behandelt.

[830] Vgl. Löwe/Rosenberg-*Schäfer,* § 96 Rn. 28.

[831] Vgl. SK-StPO-*Wohlers,* § 96 Rn. 18.

[832] Vgl. KK-*Nack,* § 96 Rn. 16.

[833] Vgl. SK-StPO-*Wohlers,* § 96 Rn. 18.

[834] Vgl. die § 2 I 2 BVerfSchG, § 1 I 1 BNDG und § 1 I MADG; vgl. hierzu *Kornblum,* S. 173; *Soiné,* NStZ 2007, Fn. 37.

[835] Vgl. Radtke/Hohmann-*Joecks,* § 96 Rn. 15.

werden kann.[836] Die Begründung muss eine hinreichende Auseinandersetzung mit den widerstreitenden Interessen durch die oberste Dienstbehörde erkennen lassen. Diese sollte dem Gericht die Weigerungsgründe insoweit verständlich machen, damit dieses etwaige Hindernisse beseitigen und die Zurverfügungstellung des Beweismittels ermöglichen kann.[837] Die für die Geheimhaltung sprechenden Gründe sind allerdings nur insoweit zu offenbaren, als dies im Rahmen der Geheimhaltungsinteressen möglich ist.[838] In diesem Fall müssen allerdings die Gründe angeführt werden, die einer hinreichend konkreten Darlegung entgegenstehen.

(γ) Verfahrensablauf

In verfahrensrechtlicher Hinsicht werden bei einer Sperrerklärung vier Verfahrensschritte durchlaufen. In einem ersten Schritt wendet sich das Gericht mit seinem Auskunftsverlangen an die Stelle, welche die Beweisgegenstände verwahrt.[839] Dies sind im vorliegenden Fall die Nachrichtendienste. Die ersuchte Behörde führt in einem zweiten Schritt die Entscheidung ihrer Aufsichtsbehörde herbei. Die Sperrerklärung wird folglich nicht durch das mit der Sache befasste Gericht, sondern durch die verwahrende Behörde eingeholt.[840] In dieser Phase entscheidet die oberste Dienstbehörde anhand bestimmter Kriterien, ob die Auskunft erteilt werden darf oder ob eine Sperrerklärung abzugeben ist. Kommt die Behörde nach einer Abwägung zu der Auffassung, dass eine Sperrung notwendig ist, ist diese Entscheidung dem Gericht in einem dritten Schritt mit der erforderlichen Begründung mitzuteilen. In einem vierten Schritt überprüft das Gericht die Rechtmäßigkeit der Sperrerklärung. Hierbei nimmt es nach überwiegender Ansicht eine bloße Plausibilitätskontrolle vor.[841] Hält das Gericht die Begründung für unzureichend, lässt sie der obersten Dienstbehörde eine Gegenvorstellung zukommen. Durch diese muss das Gericht versuchen auf die Aufhebung der Sperrerklärung hinzuwirken, um eine Aufklärungsrüge im Revisionsverfahren zu verhindern. Je nach Entscheidung der obersten Dienstbehörde wird dem Begehren stattgegeben oder die Sperrerklärung aufrechterhalten.

---

836 Vgl. Beschluss des BVerwG vom 19.4.2010, Az. BVerwG 20 F 13.09.

837 Vgl. KK-*Nack,* § 96 Rn. 17; Graf-*Ritzert,* § 96 Rn. 6.

838 Vgl. KK-*Nack,* § 96 Rn. 17.

839 Vgl. Löwe/Rosenberg-*Schäfer,* § 96 Rn. 53.

840 Vgl. LG Darmstadt NStZ 1989, S. 86f, sowie Löwe/Rosenberg-*Schäfer,* § 96 Rn. 75; SK-StPO-*Wohlers,* § 96 Rn. 20.

841 Der Sperrerklärung liegt eine Risikoeinschätzung zugrunde, die der entscheidenden Behörde ausnahmsweise einen Beurteilungsspielraum einräumt; vgl. BVerfG NJW 1981, S. 1719, 1725; OLG Hamm NStZ 1985, S. 566; Graf-*Ritzert,* § 96 Rn. 6. Kritisch dazu SK-StPO-*Wohlers,* § 96 Rn. 32f. Für eine uneingeschränkte Kontrolle OLG Stuttgart NJW 1991, S. 1971f; OLG Frankfurt StV 1983, S. 53f. Unstreitig ist dagegen die Prüfungspflicht nach § 244 II StPO.

(δ) Taugliche Sperrobjekte

In materieller Hinsicht fordert § 96 StPO das Vorliegen eines tauglichen Sperrobjekts. Ausdrücklich erfasst werden lediglich Akten oder andere in amtlicher Verwahrung befindliche Schriftstücke. Der Begriff der Schriftstücke ist jedoch weit auszulegen und erstreckt sich nach allgemeiner Ansicht zusätzlich auf Ton- und Bildträger, Abbildungen, Filme, elektronische Datensätze oder sonstige Beweisgegenstände, sofern ein vergleichbares Geheimhaltungsbedürfnis besteht.[842] Nach gefestigter Rechtsprechung ist die Vorschrift des § 96 StPO zudem analog auf Auskünfte über Name und Identität eines Zeugen anwendbar.[843] Diese Analogie wird mit dem vergleichbaren Gefährdungspotential beziehungsweise Schutzbedürfnis begründet.[844] Die Verpflichtung der Behörde zur Erteilung einer Auskunft kann nicht weiter gehen, als diejenige zur Vorlegung von Akten.[845] Zudem wird hierdurch einheitlich die Zuständigkeit der obersten Dienstbehörde begründet. Diese Analogie ist selbst für Verdeckte Ermittler der Nachrichtendienste erforderlich, da die Vorschrift des § 110b III StPO nur im Strafverfolgungssektor anwendbar ist.[846] Auf der Grundlage des § 96 StPO können daher sowohl Akten als auch Zeugen gesperrt werden.[847]

(ε) Taugliche Geheimhaltungsgründe

Weiterhin muss ein ausreichender Geheimhaltungsgrund vorliegen. Nach § 96 StPO muss das Bekanntwerden des Inhalts dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten. Unstreitig anerkannt wurde ein ausreichendes Schutzbedürfnis für die Geheimhaltung von Staatsgeheimnissen, die Bestands- und Funktionsfähigkeit der genannten Gebietskörperschaften sowie Staatsangelegenheiten von außenpolitischer und militärischer Bedeutung.[848] Die Bekämpfung und Aufklärung schwerwiegender Straftaten wurde ebenfalls als ausreichender Geheim-

---

842 Vgl. Graf-*Ritzert,* § 96 Rn. 1; KK-*Nack,* § 96 Rn. 6; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 42; Radtke/Hohmann-*Joecks,* § 96 Rn. 5ff; SK-StPO-*Wohlers,* § 96 Rn. 4.

843 Vgl. BVerfG NJW 1981, S. 1719, 1723; BGH NJW 1981, S. 1052; *Eisenberg,* Rn. 1267; *Kornblum,* S. 177; KK-*Nack,* § 96 Rn. 6; Löwe/Rosenberg-*Schäfer,* § 96 Rn.44, 61; *Zacharias,* S. 298.

844 Zur Zulässigkeit einer Sperrerklärung bei Lebensgefahr BGH NJW 1981, S. 1052, sowie insgesamt OLG Hamburg StV 1981, S. 537ff.

845 Vgl. OLG Hamm NStZ 1990, S. 44f.

846 Vgl. *Kornblum,* S. 177.

847 Eine Heranziehung des § 54 StPO wird überwiegend nicht mehr für erforderlich gehalten, vgl. Graf-*Ritzert,* § 96 Rn. 1; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 44. Der Verweigerung der Aussagegenehmigung nach § 54 StPO kommt eine eigenständige Bedeutung daher nur bei Bekundungen von Zeugen zu, die nicht schriftlich fixiert vorliegen.

848 Vgl. BVerwG NJW 2010, S. 2295f; VG Weimar NVwZ-RR 2002, S. 394f, sowie *H. Müller,* Geheimhaltung, S. 26f.

haltungsgrund angesehen.[849] Erfasst sind dabei vor allem Straftaten, die die innere und äußere Sicherheit des Staates bedrohen, schwerwiegende Fälle des Rauschgifthandels oder Kapitalverbrechen.[850]

Wann in den übrigen Fällen ein ausreichender Geheimhaltungsgrund vorliegt, wird unterschiedlich beantwortet. Ein erster Streitpunkt betrifft die Einbeziehung von Individualinteressen. Diese werden verschiedentlich unter Verweis auf den Wortlaut des § 96 StPO abgelehnt, der auf eine Beeinträchtigung von Bundes- oder Landesinteressen und damit auf Gemeinwohlbelange abstelle.[851] Diese Ansicht verkennt jedoch die Schutzpflichten des Staates. Diese können richtigerweise bei einer konkreten Gefährdung von Leben, Gesundheit oder Freiheit eine Sperrerklärung rechtfertigen.[852] Voraussetzung ist jedoch, dass eine derartige Bedrohung ernstlich zu befürchten ist.[853]

Ebenfalls streitig ist, inwiefern die künftige Verwendbarkeit einer Informationsquelle als Geheimhaltungsgrund ausreicht. Abseits der Regelung für den strafprozessualen Ermittler nach § 110b III 3 StPO wurde eine Verwendungsgefährdung als Sperrgrund nicht ausdrücklich festgeschrieben. Fraglich ist daher, ob dieser Geheimhaltungsgrund auf andere Ermittlungspersonen der Nachrichtendienste ausgeweitet werden kann. Die Diskussion zur Verwendungsgefährdung fokussiert sich überwiegend auf Informanten der Strafverfolgungsbehörden, allerdings lassen sich die Argumente weitgehend auf Ermittlungspersonen der Nachrichtendienste übertragen. Nach dem ausdrücklichen Willen des Gesetzes verbürgt die Vorschrift des § 110b III 3 StPO einen allgemeinen Rechtsgedanken, demzufolge die Verwendungsgefährdung von Auskunftspersonen insgesamt einen ausreichenden Geheimhaltungsgrund darstellt.[854] Diese Wertung wird von der überwiegenden[855] Ansicht

---

[849] Die hierzu ergangene Rechtsprechung und Literatur ist allerdings uneinheitlich, vgl. Radtke/Hohmann-*Joecks,* § 96 Rn. 14; KK-*Nack,* § 96 Rn. 18, 23. Kritisch dazu *H. Müller,* Geheimhaltung, S. 27ff; SK-StPO-*Wohlers,* § 96 Rn. 23.

[850] So etwa VGH Mannheim NJW 1991, S. 2097f; OLG Stuttgart NJW 1991, S. 1071f; OLG Hamburg StV 1981, S. 537f. Ablehnend SK-StPO-*Wohlers,* § 96 Rn. 23. Der BGH fordert für die Annahme der „Unerreichbarkeit" zusätzlich eine Leibes- oder Lebensgefahr, vgl. etwa BGH NJW 1985, S. 984, 986.

[851] Vgl. SK-StPO-*Wohlers,* § 96 Rn. 22.

[852] Vgl. BVerfGE 57, 250, 285, BGHSt 35, 164; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 58; SK-StPO-*Wohlers,* § 96 Rn. 26; *Zacharias,* S. 298f. Ebenso *Arloth,* NStZ 1993, S. 468, unter Verweis auf die Neufassung des § 68 III 1 StPO als Auslegungshilfe.

[853] So etwa Radtke/Hohmann-*Joecks,* § 96 Rn. 15.

[854] So ausdrücklich BT-Drs. 12/989, S. 42.

[855] Nach Ansicht einzelner Gegenstimmen handelt es sich bei § 110b III 3 StPO um eine allein für VE geltende Sonderregelung, die sich nur aufgrund des besonderen Aufwands von deren Einschleusung bzw. Stellung rechtfertige, vgl. SK-StPO-*Wohlers,* § 96 Rn. 25. Allerdings macht auch diese Ansicht bei unersetzbaren Geheimnisträgern eine Ausnahme, vgl. Rn. 1036.

in der Wissenschaft bestätigt.[856] Eine Übertragung auf andere Auskunfts- und Ermittlungspersonen ist damit ausdrücklich anzuerkennen.

(ζ) Verhältnismäßigkeitsgrundsatz

Als dritte materielle Voraussetzung muss eine Sperrerklärung schließlich dem Verhältnismäßigkeitsgrundsatz genügen. Die oberste Dienstbehörde darf beim Vorliegen eines Nachteils i.S.d. § 96 StPO nicht unreflektiert eine Sperrerklärung abgeben, sondern ist zur Abwägung der gesamten Umstände unter Einbeziehung der infrage stehenden Rechtsgüter und Interessen verpflichtet.[857] Die Sperrerklärung muss zur Erreichung des Geheimnisschutzes geeignet, erforderlich und angemessen sein.[858] An der Geeignetheit kann es beispielsweise fehlen, wenn die Identität des Zeugen oder der zu sperrende Akteninhalt den Beteiligten bereits aus anderen Quellen bekannt ist.[859] Hinsichtlich der Erforderlichkeit muss die oberste Dienstbehörde nachprüfen, ob mildere Schutzvorkehrungen die Geheimhaltungsinteressen in gleicher Weise effektiv schützen können und die Offenlegungs- und Verteidigungsinteressen weniger gravierend beeinträchtigen. Der Gesetzgeber hat zu diesem Zweck in den §§ 58a, 68 III, IV, 247a, 255a StPO ein abgestuftes System geschaffen, welches zum Beispiel in Bezug auf einen schutzbedürftigen Zeugen eine persönliche Vernehmung unter Wahrung bestimmter Schutzvorkehrungen ermöglicht. Sobald diese Maßnahmen zum Geheimhaltungsschutz ausreichen, ist die Sperrerklärung auf dieses Maß zu beschränken.[860] Im Rahmen der Angemessenheitsprüfung ist schließlich der Ausnahmecharakter einer staatlich verkürzten Beweisgrundlage zu berücksichtigen.[861] Die in der Abwägung heranzuziehenden Kriterien sollen einen angemessenen Ausgleich zwischen den Geheimhaltungsinteressen des Staates und der Aufklärungspflicht des Gerichts herstellen und können damit einer vollständigen Sperrung entgegenstehen.[862] Diese Kriterien betreffen die Schwere der Straftat, das Ausmaß der dem Beschuldigten drohenden Nachteile, das Gewicht der die Geheimhaltung begründenden Umstände und den Stellenwert des angestrebten Beweismittels.[863]

---

856 Vgl. stellvertretend *Meyer-Goßner*, § 96 Rn. 13.

857 Vgl. KK-*Nack,* § 96 Rn. 18.

858 Vgl. Radtke/Hohmann-*Joecks,* § 96 Rn. 16.

859 So SK-StPO-*Wohlers,* § 96 Rn. 28.

860 Vgl. *Tiedemann/Sieber,* NJW 1984, S. 754.

861 Zum Ausnahmecharakter der Sperrerklärung vgl. BGH NStZ 2005, S. 43.

862 Vgl. OLG Stuttgart NJW 1991, S. 1071f; *Droste,* Handbuch, S. 596. Vertiefend zur Abwägung vgl. KK-*Nack,* § 96 Rn. 18.

863 Vgl. BGH Urt. vom 15.9.1982 – 2 StR 765/81; OLG Celle NStZ 1983, S. 570; OLG Stuttgart NJW 1991, S. 1071f; Vertiefend bei *Droste,* Handbuch, S. 596; *H. Müller,* Geheimhaltung, S. 34.

Diese Abwägungsentscheidung soll die in Geheimhaltungsfragen widerstreitenden Interessen in einen angemessenen Ausgleich bringen.[864] Die kompensierende Wirkung der angewendeten Kriterien wird jedoch teilweise infrage gestellt. Nach Ansicht der Kritiker könne eine geringe Tatschwere beispielsweise sowohl als Begründung für eine Geheimhaltung als auch für eine Offenlegung herangezogen werden.[865] Die Einschätzung des Stellenwerts des Beweismittels sei ebenfalls problematisch, da die oberste Dienstbehörde oftmals aus tatsächlichen Gründen nicht in der Lage sei, die Bedeutung des Beweismittels für das Strafverfahren richtig und neutral zu beurteilen.[866] Erläuternde Mitteilungen vonseiten des Gerichts seien in diesem Fall ebensowenig hilfreich, da derartige Einschätzungen eine unzulässige richterliche Beweisantizipation darstellen würden.[867] Die behördliche Entscheidung sei damit fehleranfällig.[868] Die genannten Kriterien könnten eine Überbewertung staatlicher Schutzinteressen nicht verhindern, sodass Informationen gegebenenfalls häufiger als notwendig als geheimhaltungsbedürftig eingestuft würden.

(2) Auswirkungen auf das Strafverfahren

Wurden die vorgenannten Voraussetzungen erfüllt, ist die oberste Dienstbehörde zur Abgabe einer Sperrerklärung berechtigt. Diese Geheimhaltung ist mit verschiedenen Konsequenzen verbunden. Neben den unmittelbaren Rechtsfolgen wird zusätzlich auf die mit einer Sperrerklärung verbundenen gesetzlichen beziehungsweise richterlichen Kontrollsysteme und Ersatzstrategien eingegangen.

(α) Bindungswirkung und Kontrolle

Als erste Konsequenz führt eine wirksame Sperrerklärung zu einer umfassenden Bindungswirkung. Danach muss das Gericht die Sperrung trotz seiner unter Umständen gegenteiligen Auffassung akzeptieren.[869] Da es sich bei der Sperrerklärung um einen Verwaltungsakt handelt, bleibt diese Bindungswirkung selbst bei einer unberechtigten oder sonst rechtswidrigen Sperrerklärung bestehen.[870] Bei Verwaltungsakten ist insofern zwischen der Rechtmäßigkeit und der Rechtswirksamkeit zu unterscheiden. Die Rechtswidrigkeit eines Verwaltungsaktes hat nicht zwangsläufig dessen Nichtigkeit zur Folge. Fehler im Verwaltungsakt führen nur in den

---

[864] Vgl. *H. Müller,* Geheimhaltung, S. 34.

[865] Zu diesem Dilemma vgl. *H. Müller,* Geheimhaltung, S. 34f. Pro Geheimhaltung BGHSt 31, 290, 295, pro Offenlegung OLG Celle NStZ 1983, S. 570f.

[866] Vertiefend zur Fehleranfälligkeit *H. Müller,* Geheimhaltung, S. 36f m.w.N.

[867] Vgl. allgemein zur Beweisantizipation *Eisenberg,* Rn. 198.

[868] Vgl. *Weigend,* DJT, C 40.

[869] So KK-*Senge,* Vor § 48 Rn. 63.

[870] Vgl. BGH NStZ 1989, S. 380f; KK-*Senge,* Vor § 48 Rn. 63.

Fällen des § 44 VwVfG zur Nichtigkeit. Demnach bleibt die Sperrerklärung wirksam, solange sie nicht wegen besonders schwerwiegenden Fehlern nichtig und daher unbeachtlich ist. Eine Sperrerklärung kann folglich erst übergangen werden, wenn die Begründung offensichtlich willkürlich, missbräuchlich oder fehlerhaft ist.[871] Hiervon ist beispielsweise auszugehen, wenn nachweislich keine Abwägung vorgenommen wurde oder die Entscheidung auf einer offensichtlich fehlerhaften Tatsachenbasis oder Rechtsauffassung beruht. In diesem Fall ist die Sperrerklärung unwirksam, sodass das Gericht die Beschlagnahme der Akten erwirken kann.[872] Aufgrund der limitierten Prüfungskompetenz wird den Gerichten in der Praxis ein solcher Willkürnachweis allerdings nur selten gelingen.[873]

In der Konsequenz ist eine Sperrerklärung daher regelmäßig mit einer Bindung des Strafgerichts verbunden, welche letztlich zu einer vollumfänglichen Geheimhaltung der nachrichtendienstlichen Erkenntnisse führen kann. Das Gericht bleibt als Folge der richterlichen Aufklärungspflicht jedoch weiterhin im Rahmen des Möglichen zu einer erschöpfenden Sachverhaltsaufklärung verpflichtet.[874] Erhält es in diesem Zusammenhang anderweitig Kenntnis von gesperrten Akteninhalten, dürfen diese Erkenntnisse trotz der Sperrerklärung verwertet werden.[875]

Entgegen den rechtlichen Vorgaben werden die vorgenannten Beschränkungen des Strafgerichts zum Teil erheblich kritisiert. Die Kritik betrifft vor allem den auf eine Plausibilitätskontrolle festgelegten *Überprüfungsmaßstab*. Unter diesen Voraussetzungen sei das Gericht nur selten in der Lage, den für die Unwirksamkeit erforderlichen Nachweis einer willkürlichen oder grob fehlerhaften Entscheidung zu erbringen.[876] Die Überprüfung sei zusätzlich dadurch erschwert, dass die behördliche Begründung ihrerseits der Geheimhaltung unterliegen könne. Aufgrund der ohnehin geringen Erfolgsaussichten einer Gegenvorstellung sei die Effektivität der gerichtlichen Kontrolle zudem erheblich gemindert.[877]

Diese Bedenken werden von *verfassungsrechtlicher* Seite ergänzt. Bei einer vollumfänglichen Sperrung haben weder der Angeklagte noch das Strafgericht Zugang zu den verfahrensrelevanten Tatsachen. Hierdurch wird nicht nur die Garantie

---

[871] Vgl. BGH NStZ 1989, S. 380f; KG Berlin NStZ 1989, S. 541f; SK-StPO-*Wohlers,* § 96 Rn. 38ff.

[872] Vgl. BGH NJW 1992, S. 1973f; KG Berlin NStZ 1989, S. 541f; SK-StPO-*Wohlers,* § 96 Rn. 38ff.

[873] Vgl. KK-*Senge,* Vor § 48 Rn. 64.

[874] Allerdings kann ein Verzicht auf die dem Gericht obliegende Fürsorgepflicht gestützt werden.

[875] Eine Sperrerklärung begründet insofern kein Verwertungsverbot. Eine Beschlagnahme der gesperrten Akten ist indes nicht möglich, vgl. SK-StPO-*Wohlers,* § 96 Rn. 41.

[876] Vgl. BGHSt 36, S. 159, 163; BVerwG NJW 1987, S. 202, 204; *Gaede,* StV 2006, S. 602; Graf-*Ritzert,* § 96 Rn. 6; SK-StPO-*Wohlers,* § 96 Rn. 32f.

[877] Vgl. *Weigend,* DJT, C 40.

eines effektiven Rechtsschutzes i.S.d. Art. 19 IV GG, sondern auch die richterliche Unabhängigkeit selbst infrage gestellt.[878] Im Grundsatz müssen die Gerichte frei entscheiden können, welche Beweismittel sie für eine Sachaufklärung für notwendig erachten und welche nicht.[879] Bei einer Sperrerklärung wird diese Entscheidungsbefugnis geschmälert und das Gericht durch die Exekutive auf ein sachferneres Beweismittel verwiesen. Durch die Bindung der behördlichen Abwägungsentscheidung wirkt die Exekutive letztlich in den richterlichen Kompetenzbereich hinein. Hiervon kann nur in Fällen von Willkür abgewichen werden. Zwar ist es richtig, dass zwingende Sachgründe das Gebot der gerichtlichen Wahrheitsfindung einschränken können,[880] diese Einschränkung ist jedoch nur hinnehmbar, wenn die entscheidungsbefugte Behörde über das erforderliche Urteilsvermögen verfügt und gesetzliche Vorgaben die Rechtmäßigkeit einer solchen Abwägungsentscheidung sicherstellen.[881] Diese Vorgaben sind wegen der unklaren behördlichen Entscheidungskriterien nicht gewahrt. Das bei einer Sperrerklärung bestehende Übergewicht der Exekutive ist daher bedenklich. Die gerichtliche Kontrolle kann die mit der Geheimhaltung verbundenen Nachteile letztlich nur bedingt ausgleichen.[882]

Weitere Kritik wird zum Teil unter Bezugnahme auf die *Rechtsprechung des EGMR* geäußert. Dieser verlange bei der Heranziehung anonymer Zeugenaussagen eine uneingeschränkte gerichtliche Überprüfbarkeit.[883] Das Verbot einer Plausibilitätskontrolle wird allerdings zu Unrecht auf das deutsche Lösungsmodell übertragen. In den vom EGMR behandelten Fällen wurde die anonyme Zeugenaussage als ausschließliches Beweismittel herangezogen. Eine solche, einzig auf Angaben einer anonymen Gewährsperson gestützte Entscheidungsgrundlage ist im deutschen Recht nicht zulässig.[884] Hier ist vielmehr eine Bestätigung durch weitere Beweiszeichen erforderlich. Im Übrigen ist die Verwertbarkeit von Beweismittel vorrangig den Regeln des innerstaatlichen Rechts überlassen, soweit die dortigen Regeln die Fairness des Verfahrens in seiner Gesamtheit gewährleisten können.[885] Ausgehend von dieser Prämisse kommt den nachfolgend beschriebenen Kompensationsmechanismen eine erhebliche Bedeutung zu.

---

[878] So *H. Müller,* Geheimhaltung, S. 39. *Wattenberg,* StV, S. 695, spricht von einer „bloßen Missbrauchskontrolle auf lückenhafter Tatsachenbasis".

[879] So *Detter,* NStZ 2003, S. 5.

[880] So *Detter,* NStZ 2003, S. 5.

[881] Vgl. BVerfG NJW 1981, S. 1719, 1725, sowie *Detter,* NStZ 2003, S. 6.

[882] Vgl. *Schnabel,* NVwZ 2010, S. 881.

[883] So *Gaede,* StraFo 2004, S. 197; *Gaede,* StV 2006, S. 604; SK-StPO-*Wohlers,* § 96 Rn. 34.

[884] Vgl. BGH NJW 2000, S. 1661f; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 80.

[885] Vgl. BGH NJW 2000, S. 1661f.

(β) Unerreichbarkeit und Beweissurrogation

Als zweite Konsequenz führt eine wirksame Sperrerklärung zur Unerreichbarkeit des gesperrten Beweismittels i.S.d. §§ 251, 244, 223 StPO und eröffnet dadurch die Möglichkeit einer Beweissurrogation.[886] Als taugliche Beweissurrogate haben sich die Verlesung von polizeilichen Niederschriften, die schriftliche Befragung mittels Fragenkatalog, die Vernehmung eines mittelbaren Zeugen sowie eine audiovisuelle Vernehmung bewährt.[887] Schließlich ist eine Verlesung von Behördenzeugnissen nach § 256 I Nr. 1a StPO denkbar, da die Nachrichtendienste als öffentliche Behörden derartige Zeugnisse zur Verfügung stellen können.[888] Überwiegend werden jedoch die Einführung des Hörensagenbeweises sowie die Verlesung von Behördenzeugnissen favorisiert.[889] Die Vernehmung von Verhörpersonen als Zeugen vom Hörensagen kommt in Betracht, wenn der Zeuge infolge der Sperrung selbst nicht in der Hauptverhandlung aussagen kann. Sofern sich die Sperrerklärung nicht zugleich auf die Vernehmungsunterlagen erstreckt, können die Aussagen des Zeugen vermittelt über den polizeilichen Vernehmungsbeamten oder Vernehmungsprotokolle eingeführt werden.[890]

Im deutschen Recht ist die Beweissurrogation die zentrale Ersatzstrategie, um die Nutzung geheimhaltungsbedürftiger Erkenntnisse zu ermöglichen. Die Beweissurrogation soll dabei die mit einer Geheimhaltung verbundenen Nachteile kompensieren.[891] Gegen diesen Lösungsansatz werden vor allem Bedenken in Bezug auf die Grundsätze des Strafverfahrens angeführt.

Ein erster Kritikpunkt betrifft den Grundsatz der *Unmittelbarkeit*. Dieser Grundsatz gebietet grundsätzlich die Heranziehung des sachnächsten Beweismittels, was in Bezug auf gesperrte Beweismittel nicht unbedingt möglich ist. Dennoch scheidet in den meisten Fällen eine Verletzung des in §§ 249, 250 StPO statuierten Unmittelbarkeitsgrundsatzes aus. Ein Beispiel ist etwa der Zeuge vom Hörensagen.

---

[886] Vgl. *Meyer-Goßner*, § 96 Rn. 10; KK-*Nack,* § 96 Rn. 12. Etwas anderes gilt nur im Fall einer willkürlichen Sperrerklärung, vgl. Löwe/Rosenberg-*Schäfer,* § 96 Rn. 94. Zur Surrogation vgl. *Zacharias,* S. 305ff. In der Wissenschaft wird jedoch der Rückgriff auf Surrogate zum Teil generell nur bei rechtswidriger Sperrung ausgeschlossen. Andere wollen entlastende Tatsachen zudem als wahr unterstellen. Eine Übersicht zum Meinungsstand findet sich bei Löwe/Rosenberg-*Schäfer,* § 96 Rn. 84ff, 97.

[887] Vgl. zu den einzelnen Surrogaten u.a. BGHSt 33, 70; BGH NStZ 2001, S. 212; BGH NStZ 1993, S. 292; BGH NStZ-RR 2002, S. 176 sowie *Detter,* NStZ 2003, S. 6; *Detter,* StV 2006, S. 544ff; *Zacharias,* S. 305ff.

[888] Vgl. *Droste,* Handbuch, S. 590; KK-*Diemer,* § 256 Rn. 4; *Soiné,* NStZ 2007, S. 252.

[889] Vgl. BVerfG NJW 1996, S. 448f; BVerfG NJW 1981, S. 1719, 1726f.

[890] Vgl. hierzu beispielsweise BGH NStZ-RR 2002, S. 176; BVerfG NJW 1996, S. 448; *Soiné,* NStZ 2007, S. 252. Zur Erstreckung der Sperrerklärung auf sonstige Unterlagen BGH 3 StR 218/03 – Urteil vom 4. März 2004, sowie *Tiedemann/Sieber,* NJW 1984, S. 754.

[891] Vgl. *Norouzi,* JuS 2003, S. 435.

Obwohl dieser nicht selbst am Geschehen beteiligt war, kann er in Bezug auf die Aussagen des Dritten unmittelbar über seine eigene Wahrnehmung berichten. Der im Unmittelbarkeitsgrundsatz verbürgte Vorrang des Personalbeweises vor dem Urkundsbeweis wird hierdurch nicht beeinträchtigt.[892] In Bezug auf die Verlesung von Vernehmungsprotokollen hat der Gesetzgeber in den §§ 251ff StPO zudem selbst eine Abwägung getroffen, nach der angesichts des sonst drohenden Beweisverlustes eine Abweichung vom Grundsatz der Unmittelbarkeit ausnahmsweise zulässig ist.[893] Steht das unmittelbare Beweismittel im Fall einer Sperrerklärung auf absehbare Zeit nicht zur Verfügung, muss der Richter den Sachverhalt mit den ihm verbleibenden Möglichkeiten aufklären können. Soweit die in der Strafprozessordnung anerkannten Ausnahmefälle beachtet werden, ist die im Zuge einer Sperrerklärung erfolgende Beweissurrogation unter dem Aspekt der Unmittelbarkeit nicht zu beanstanden.[894] Bei der Nutzung von Geheimdienstinformationen ergeben sich diesbezüglich keine Besonderheiten.

Ein zweiter Kritikpunkt betrifft die Vereinbarkeit mit der *richterlichen Aufklärungspflicht* nach § 244 II StPO.[895] Diese verpflichtet das Gericht zur erschöpfenden Sachverhaltsaufklärung unter Heranziehung der sachnächsten und bestmöglichen Beweismittel.[896] Diese Aufgabe wird erheblich erschwert, wenn beispielsweise Auskünfte über Name und Anschrift des Gewährsmannes verweigert werden. Ein Verstoß gegen die Aufklärungspflicht scheidet bei einer Sperrerklärung nur aus, wenn das Gericht neben der Gegenvorstellung alle sonst denkbaren Anstrengungen unternommen hat, um auf eine Aufhebung der Sperrerklärung hinzuwirken oder das Beweismittel auf anderem Wege zu erhalten.[897] Erst wenn das Beweismittel trotz Ausschöpfung aller Einwirkungsmöglichkeiten in absehbarer Zeit nicht verfügbar ist, ist eine mittelbare Beweisführung unter dem Aspekt der Aufklärungspflicht unbedenklich.[898] Die Wahrung der richterlichen Aufklärungspflicht hängt damit vor allem von den durch das Gericht unternommenen Bemühungen ab. Dies ist jedoch rechtlich unbedenklich, da durch die richterliche Aufklärungspflicht ein solches Tätigwerden gesetzlich abgesichert ist.

---

892 Vgl. BGHSt 6, 209, 1. Leitsatz; BGHSt 17, 382f; *Roxin/Schünemann*, § 46 Rn. 33ff.

893 Die Durchbrechung der Unmittelbarkeit durch die Vorschrift des § 251 fügt sich in eine Entwicklung ein, die durch eine zunehmende Relativierung des Unmittelbarkeitsgrundsatzes geprägt ist. Kannte die RStPO von 1877 noch ein absolutes Verlesungsverbot, so wird dieses Prinzip zunehmend aufgeweicht und damit selbst zur Ausnahme; vgl. vertiefend *Großkopf,* S. 20ff, 51.

894 Vertiefend *Roxin/Schünemann*, § 46 Rn. 3ff.

895 Kritisch *Roxin/Schünemann*, § 46 Rn. 33f.

896 Vgl. BGH NStZ 2004, S. 50; BGH NJW 2000, S. 2517, 2518; *Eisenberg,* Rn. 1031.

897 Vgl. zur Aussagegenehmigung BGHSt 17, 382, 384.

898 Vgl. BGH NStZ 2004, S. 50, sowie *Eisenberg,* Rn. 1031.

Daneben wird die Verletzung des *Fragerechts* aus § 240 II StPO, Art. 6 III lit. d EMRK gerügt.[899] Dieses gewährleistet dem Angeklagten ein umfassendes „Recht auf Verteidigung".[900] Er muss grundsätzlich direkte Fragen an den (Belastungs-)Zeugen stellen dürfen, um dadurch dessen Glaubwürdigkeit testen und zur Ermittlung des wahren Sachverhalts beitragen zu können.[901] Allerdings bezieht sich der Anwendungsbereich des § 240 II StPO nur auf den in der Hauptverhandlung *anwesenden* Zeugen.[902] Solange die Verhörperson als Zeuge vom Hörensagen uneingeschränkt befragt werden kann, scheidet die Verletzung des Fragerechts aus.[903] Ebenso verhält es sich bei der audiovisuellen Vernehmung, in deren Rahmen ohnehin eine unmittelbare Befragung des Zeugen gestattet wird.[904] Bedenken ergeben sich allerdings mit Blick auf das durch die EMRK gewährleistete Fragerecht, dem ein umfassenderer Zeugenbegriff zugrunde liegt. Der konventionsrechtliche Zeugenbegriff erstreckt sich auf sämtliche Personen, deren Wahrnehmungen für die Entscheidungsfindung von Interesse sind. Somit wird auch der im Hintergrund stehende gesperrte Zeuge erfasst.[905] In der Praxis werden diese Bedenken jedoch durch die Vorlage eines Fragekatalogs ausgeräumt.[906] Eine Verletzung des rechtlichen Gehörs scheidet in den meisten Fällen ebenfalls aus. Die zur Verwertung herangezogenen Beweissurrogate stehen allen Verfahrensbeteiligten in gleicher Weise zur Verfügung. Der mit der Sperrung verbundene Erkenntnisverlust in Bezug auf den optischen und persönlichen Eindruck einer Zeugenvernehmung betrifft alle am Verfahren Beteiligten. Im Übrigen kann der Angeklagte auf den minderen Beweiswert hinweisen und auf die Heranziehung sachnäherer Beweismittel drängen.[907] Die Heranziehung eines bestimmten Beweises oder einer bestimmten Art von Beweismittel wird durch den Anspruch auf rechtliches Gehör nicht gewährt.[908]

Weiterhin bestehen Bedenken in Bezug auf den *Beweiswert* mittelbarer Beweismittel. Bei einer Beweissurrogation bleiben wesentliche Erkenntnisse verschlossen, die zur Beurteilung der Glaubwürdigkeit erforderlich sind. Oftmals kann eine aussagekräftige Einschätzung erst durch die persönliche, unmittelbare Wahrnehmung getroffen werden. Der Beweiswert eines Zeugenbeweises wird insofern nicht nur vom Inhalt des Gesagten, sondern maßgeblich vom persönlichen Eindruck des

---

899 Vgl. zu dieser Frage *Eisenberg,* Rn. 797a; *Zacharias,* S. 313f.

900 So *Eisenberg,* Rn. 792.

901 Vgl. *Eisenberg,* Rn. 792; *Pfeiffer* StPO, § 240 Rn. 1; KK-*Schneider,* § 240 Rn. 1.

902 Vgl. *Eisenberg,* Rn. 1032.

903 Vgl. BGH NJW 1962, S. 1876f.

904 Hierzu u.a. BGH NStZ 2004, S. 345ff sowie Widmaier, § 18 Rn. 23.

905 Vgl. EGMR StV 1992, S. 499f; BGH NStZ 1993, S. 292, sowie *Zacharias,* S. 35.

906 Vgl. *Zacharias,* S. 314. Zur Zulässigkeit und Notwendigkeit dieses Mittels vgl. BGH NStZ 1993, S. 292.

907 Vgl. BVerfG NJW 1981, S. 1719, 1721.

908 Vgl. BVerfG NJW 1981, S. 1719, 1722; BVerfG NJW 1983, S. 1043; ebenso *Eisenberg,* Rn. 1049.

Zeugen, seiner Körpersprache und seinem Gesprächsverhalten beeinflusst.[909] Bei einer Beweissurrogation spielt schließlich neben der ursprünglichen Quelle zusätzlich die Zuverlässigkeit des Beweismittlers eine erhebliche Rolle, da die Fehleranfälligkeit eines Beweismittels mit der Anzahl der Zwischenglieder in der Beweisführung steigt.[910] Insbesondere bei der Vernehmung einer Verhörperson besteht die Gefahr, dass die Aussagen unbewusst durch die eigene berufsbezogene Wahrnehmung gefiltert werden.[911] Die Protokollverlesung ist vergleichbar bedenklich, da der Beweiswert eines Protokolls durch Fehler bei der Protokollerstellung erheblich gemindert werden kann. Mögliche Fehler können sowohl auf der notwendigerweise subjektiven Wahrnehmung des Protokollierenden als auch der zusammenfassenden Darstellung im Protokoll beruhen.[912] Insbesondere eine Zusammenfassung kann nicht die gleiche Informationsdichte aufweisen wie die Vernehmung selbst. Diese Mängel muss das Gericht bei seiner Entscheidungsfindung berücksichtigen. Dem Richter steht es daher frei, den Beweiswert des Beweismittels im Rahmen der freien richterlichen Beweiswürdigung nach § 261 StPO herabzustufen.

Schließlich wird eine Beeinträchtigung der *Verfahrensfairness* befürchtet.[913] Es ist allerdings zu berücksichtigen, dass nicht jede Beeinträchtigung der Verteidigungsmöglichkeiten notwendigerweise zu einer Verletzung des Rechts auf ein faires Verfahren führt. Ein Anspruch auf eine bestmögliche oder optimale Verteidigung wird gerade nicht gewährleistet.[914] Vielmehr muss das Strafverfahren in seiner Gesamtheit den Bedingungen eines fairen Verfahrens genügen. In diese Gesamtbetrachtung sind nach Ansicht des EGMR sowohl die Beweiserhebung als auch die Beweiswürdigung mit einzubeziehen.[915] Inwiefern die Geheimhaltung ausreichend kompensiert wird, kann folglich nur im Zusammenhang mit der späteren Beweiswürdigung beantwortet werden. Mit diesem Kompensationsmechanismus setzt sich die Untersuchung im nächsten Abschnitt eingehend auseinander.

(γ) Beweiswürdigung und Beweiswert

Als dritte Konsequenz einer Sperrerklärung muss das Gericht die mit der staatlichen Geheimhaltung verbundenen Nachteile in seine Entscheidungsfindung mit einbeziehen. Die staatlichen Geheimhaltungsinteressen dürfen sich nach höchst-

---

[909] Vertiefend *Großkopf,* S. 37.

[910] Vgl. BGHSt 17, 382, 385; BVerfG NJW 1981, S. 1719, 1725; *Großkopf,* S. 35; *Gusy,* Grundrechte, S. 115; *Nagler,* in: Baden-Württembergische Strafverteidiger e.V., S. 169; KK-*Schoreit,* § 261 Rn. 29a.

[911] Vgl. *Zacharias,* S. 310.

[912] Vgl. vertiefend *Großkopf,* S. 41ff.

[913] Vgl. *Zacharias,* S. 315ff.

[914] Vgl. *Zacharias,* S. 320.

[915] Vgl. allgemein zu dieser Gesamtbetrachtung die Entscheidungen des EGMR NJW 2003, S. 2297, sowie NStZ 2007, S. 103f.

richterlicher Rechtsprechung nicht zum Nachteil des Angeklagten auswirken.[916] Die staatlich verkürzte Beweisgrundlage ist daher nach Ansicht der Rechtsprechung durch eine sogenannte vorsichtige Beweiswürdigung und die Anwendung des Zweifelssatzes zu berücksichtigen. Zwar spielt die Unerreichbarkeit eines Beweismittels bei der Beweiswürdigung grundsätzlich keine Rolle, dies ändert sich jedoch, wenn wie vorliegend nicht ein objektiver Umstand, sondern der Einfluss der Exekutive die Nutzung des Beweismittels verhindert. Nach dem Konzept der vorsichtigen Beweiswürdigung werden die mittelbaren Beweismittel einer besonders vorsichtigen und kritischen Beweiswürdigung unterzogen.[917] Da der Richter oftmals weder die Glaubwürdigkeit der Quelle noch Schwächen im Erhebungs-, Analyse- und Übermittlungsprozess hinreichend überprüfen kann, führt diese Würdigung regelmäßig zu einer Herabstufung des Beweiswerts.[918] Der im Vergleich zum unmittelbaren Beweismittel geringere Beweiswert wird am Beispiel nachrichtendienstlicher Behördenzeugnisse deutlich. Inhaltlich beziehen sich solche Zeugnisse auf amtlich festgestellte Tatsachen und Wahrnehmungen. Sie enthalten regelmäßig keine Angaben, welche die beteiligten Personen identifizieren.[919] Das Behördenzeugnis deckt dementsprechend nur Teilaspekte ab, was der Richter beweismindernd berücksichtigen wird.[920] Diese Konsequenz gilt für die Nutzung eines Zeugen von Hörensagen in gleicher Weise. Dieser berichtet lediglich über das, was ihm die unmittelbar wahrnehmende Person zuvor mitgeteilt hat.[921] Die Verlässlichkeit der Aussage sinkt mit der Anzahl der Zwischenglieder, die zwischen den aussagenden Zeugen vom Hörensagen und dem unmittelbar wahrnehmenden Dritten treten.[922] Diese im Beweiswert reduzierten mittelbaren Beweismittel dürfen zudem nicht als alleinige Entscheidungsgrundlage herangezogen werden, sondern sind in einer Gesamtschau aller Beweismittel durch weitere Beweisanzeichen zu bestätigen.[923] Kann sich das Gericht trotz Ausschöpfung aller Beweismittel nicht von der rechtswidrigen und schuldhaften Verwirklichung des gesetzlichen Tatbestands überzeugen, greift es auf einer zweiten Stufe auf den Zweifelssatz *in dubio pro reo* zurück. Sind danach weiterhin Zweifel am Bestehen bestimmter Tatsachen vorhanden, muss es den für den Angeklagten günstigsten Sachverhalt zugrunde legen und ihn gegebenenfalls freisprechen.[924] Der Zweifelssatz bildet damit das

---

916 BGH NStZ 2000, S. 265, 267.

917 Vgl. BVerfG NJW 1996, S. 448f.

918 Vgl. *Gleß,* NJW 2001, S. 3606. Die Herabstufung des Beweiswerts entspricht der Rechtsprechung des EGMR; vgl. hierzu *Wattenberg,* StV, S. 691.

919 Vgl. *Soiné,* NStZ 2007, S. 252.

920 Vgl. *Soiné,* NStZ 2007, S. 252.

921 Vgl. *Eisenberg,* Rn. 1027ff; Graf-*Eschelbach*, § 261 Rn. 53.

922 Vgl. BGH NJW 1986, S. 1766f; Graf-*Ganter,* § 250 Rn. 10.

923 Vgl. BGH NStZ 2000, S. 265, 267; BGH NStZ 2000, S. 607; BGH NStZ-RR 2002, S. 176; BVerfG NJW 1996, S. 448; BVerfG NJW 1981, S. 1719, 1725f, sowie *Detter,* NStZ 2003, S. 4; *Gleß,* NJW 2001, S. 3606.

924 Vgl. BGH NJW 1957, S. 1642f, sowie stellvertretend *Eisenberg,* Rn. 116.

abschließende Regulativ der zweistufigen Rechtsprechungslösung. Dieses Zusammenspiel von vorsichtiger Beweiswürdigung und Zweifelssatz kann nach Ansicht der Rechtsprechung die Fairness des Verfahrens in seiner Gesamtheit herstellen.[925]

Weitere Besonderheiten ergeben sich bei der Zurückhaltung entlastenden Beweismaterials. In dieser Geheimhaltungsvariante wird nicht nur die Entscheidungsgrundlage des Gerichts um ein wichtiges Beweismittel verkürzt, sondern dem Angeklagten zugleich ein unter Umständen relevanter Entlastungsbeweis entzogen.[926] In einer derartigen Konstellation greift die Beweiswürdigungslösung zu kurz, da gerade kein Beweissurrogat vorliegt, das in seinem Beweiswert herabgestuft werden kann. Dieses Defizit versucht der BGH durch eine Ergänzung der erläuterten Mechanismen zu beheben. Die vorsichtige Beweiswürdigung und der Zweifelssatz werden um ein drittes Regulativ des hypothetischen beziehungsweise fiktiven Vergleichs erweitert.[927] Dieser hypothetische Vergleich setzt sich aus drei Prüfungsschritten zusammen. In einem ersten Schritt muss der Tatrichter unterstellen, dass sich das Entlastungsvorbringen des Angeklagten ohne die Sperrung als korrekt bestätigt hätte. Dieses hypothetische Beweisergebnis muss er in einem zweiten Schritt den vorhandenen Beweisergebnissen gegenüberstellen. In einem dritten Schritt überprüft er diese beiden Ergebnisse unter Beachtung des Zweifelssatzes. Die vorhandenen Beweismittel müssen für eine Verurteilung das potentiell entlastende Vorbringen soweit entkräften, dass der Richter trotz der verkürzten Beweisgrundlage weiterhin von der Schuld des Angeklagten überzeugt ist. An diese Überzeugung sind umso höhere Anforderungen zu stellen, je näher das gesperrte Beweismittel zur Tat steht und je eher sich das hypothetische, potentiell entlastende Beweisergebnis in die bereits vorhandende Beweislage einfügt. Diese Ergänzung der vorsichtigen Beweiswürdigung um einen hypothetischen Vergleich unter Berücksichtigung des Zweifelssatzes reicht nach Ansicht des BGH aus, um die durch die Zurückhaltung der entlastenden Beweise bedingten Nachteile auszugleichen. Eine Verfahrenseinstellung hält die Rechtsprechung nur in einem extremen Ausnahmefall für notwendig. Ein solcher wäre anzunehmen, wenn bei einer Gesamtbetrachtung ein faires Verfahren unter keinem Gesichtspunkt gewährleistet werden kann.[928] Dieser Ansatz entspricht der Gesamtbetrachtung des EGMR, wonach ein

---

[925] Vgl. *Gaede,* StraFo 2004, S. 195. Vertiefend zu den allgemeinen Anforderungen an die Beweiswürdigung bei Beweissurrogaten *Zacharias,* S. 312.

[926] Vgl. hierzu den sog. *Motassadeq*-Fall in BGH NJW 2004, S. 1259. In diesem Verfahren konnte der Angeklagte eine Beteiligung an den Anschlägen vom 11.9.2001 nicht hinreichend bestreiten, da der potenzielle Entlastungszeuge B. in den USA inhaftiert war und sowohl die amerikanische als auch die deutsche Regierung jede Mitwirkung unter Hinweis auf Sicherheitsbedenken verweigerten. Letztlich wurden weder der unmittelbare Zeuge, die Vernehmungsperson noch die Vernehmungsprotokolle freigegeben. Dieser Fall bildet die Grundlage für die beschriebenen Kompensationsmechanismen.

[927] Vgl. BGH NStZ 2004, S. 343f.

[928] Allgemein zur Annahme eines Verfahrenshindernisses in außergewöhnlichen Sonderfällen vgl. BGHSt 46, S. 159, 171.

Einzelverstoß gegen Verbürgungen des *fair trial*-Grundsatzes aus Art. 6 III EMRK im Gesamtverfahren kompensiert werden kann.[929]

Eine weitere Sonderkonstellation betrifft die Geheimhaltung, die auf den Einfluss ausländischer Staaten zurückzuführen ist.[930] Derartige Sachverhalte gewinnen aufgrund des international agierenden Terrorismus zunehmend an Bedeutung, da die Nutzung nachrichtendienstlicher Erkenntnisse neben den nationalen Interessen oftmals die Arbeit ausländischer Dienste und damit die Interessen anderer Staaten betrifft.[931] Anders als in den bisherigen Geheimhaltungsvarianten handelt es sich bei einer externen Einflussnahme nicht um die sogenannte rechtliche, sondern um die tatsächliche Unmöglichkeit i.S.d. § 244 III 2 StPO. Diese wird bei der Beweiswürdigung grundsätzlich nicht berücksichtigt.[932] Eine Ausnahme gilt jedoch, wenn der ausländische Staat in Bezug auf das konkrete Strafverfahren eigene staatliche Interessen verfolgt.[933] In diesem Fall nehmen die deutschen Gerichte die Verurteilung des Täters stellvertretend für den ausländischen Staat vor. Versucht dieser Staat die deutsche Justiz zu beeinflussen, indem er etwa die Informationsübermittlung bewusst auf belastendes Beweismaterial beschränkt, ist diese selektive Rechtshilfe bei der Beweiswürdigung zu berücksichtigen. Die Rechtsprechung korrigiert in diesem Fall die Einflussnahme durch das Modell der hypothetischen Beweiswürdigung.

Der in der Rechtsprechung gefundene Ansatz der vorsichtigen beziehungsweise hypothetischen Beweiswürdigung sieht sich vonseiten der Literatur erheblicher Kritik ausgesetzt. Ein erster Kritikpunkt betrifft die praktische Handhabung der Rechtssprechungslösung. Gerade bei der Zurückhaltung entlastenden Beweismaterials sei fraglich, anhand welcher Kriterien ein Gericht einen fiktiven Beweiswert beurteilen soll.[934] Die Glaubwürdigkeitsbeurteilung eines nicht vor Gericht erscheinenden Zeugen oder eines nicht vorliegenden Sachbeweises erfordere eine hypothetische beziehungsweise fiktive Einschätzung, zu der das Gericht in der Regel nicht in der Lage sei.[935] Zudem sei unklar, wie sich eine Beweiswürdigung von einer vorsichtigen Beweiswürdigung unterscheiden solle. Da von den Richtern generell eine besondere Sorgfalt bei der Beweiswürdigung erwartet werden dürfte, seien die besonderen Anforderungen der vorsichtigen Beweiswürdigung eine bloße Beschwichtigungsformel.

---

929 Vgl. *Gleß,* NJW 2001, S. 3607; *H. Müller,* JZ 2004, S. 927.

930 Davon zu unterscheiden ist die Verwertbarkeit von Geheimdienstinformationen aus dem Ausland bzw. von ausländischen Diensten; vgl. hierzu *Rehbein,* S. 287ff, 230ff.

931 Vgl. hierzu erneut den *Motassadeq*-Fall in BGH NJW 2004, S. 1259.

932 BGHSt 49, S. 112, 124 sowie *H. Müller,* JZ 2004, S. 927.

933 Im *Motassadeq*-Fall bestand ein solches Interesse, da sich die Tat in den USA ereignete und vor allem amerikanische Bürger betroffen waren, vgl. *H. Müller,* JZ 2004, S. 927.

934 Vgl. *Detter,* StV 2006, S. 550.

935 Vgl. *Detter,* StV 2006, S. 549f; *Gröger,* S. 172; *H. Müller,* JZ 2004, S. 928.

Als zweiter Kritikpunkt wird dem Staat widersprüchliches Verhalten vorgeworfen. Da die Exekutive das Beweisdefizit selbst durch die Sperrung herbeiführe, müsste sie auch umgekehrt die Konsequenzen des Beweisausfalls tragen. Ausgehend von dieser Prämisse wird daher zum Teil gefordert, dass das Entlastungsvorbringen des Angeklagten als wahr unterstellt und sonstige Beweise einem Verwertungsverbot unterworfen werden müssten. Konkret wird die Wahrunterstellung auf die Vorschrift des § 244 III 2 StPO beziehungsweise den Zweifelssatz gestützt.[936] Das Konzept der Wahrunterstellung wird vom BGH jedoch zu Recht abgelehnt.[937] Der Zweifelssatz kommt erst zur Anwendung, wenn nach der Würdigung aller Umstände kein eindeutiges Ergebnis erzielt werden kann.[938] Eine der Gesamtwürdigung des Beweisstoffes vorgelagerte, isolierte Anwendung des Zweifelssatzes auf einzelne Elemente der Beweiswürdigung ist nicht möglich.[939] Die Gegenansicht verkennt letztlich den Charakter des Zweifelssatzes als Entscheidungsregel und deutet ihn in eine Beweisregel um.[940] Davon abgesehen existiert in der Beweislehre kein Grundsatz, wonach widersprüchliches Verhalten ein Beweisverbot begründet. Schließlich verweist die Rechtsprechung darauf, dass das Modell der Wahrunterstellung dem Angeklagten unerwünschte Einflussmöglichkeiten verschaffen würde, da dieser durch schlichte Behauptungen oder Bedrohungen des Zeugen eine Sperrerklärung und damit den Ausschluss des Beweismittels erwirken könnte.[941]

Schließlich wird vereinzelt der Anwendungszeitpunkt der Beweiswürdigungslösung kritisiert. Dieser setze unter Berücksichtigung der EGMR-Rechtsprechung zu spät an.[942] Die bei einer Geheimhaltung erforderliche Abwägung sei grundsätzlich durch die Justiz und nicht die strafverfolgende Exekutive zu treffen.[943] Die auf eine Willkürkontrolle begrenzte Prüfungskompetenz könne somit durch die nachträgliche Beweiswürdigung nicht ausgeglichen werden. Wie bereits zuvor greift die Übertragung der EGMR-Rechtsprechung mangels Vergleichbarkeit mit dem deutschen Lösungsmodell zu kurz. Die Rechtsprechung des EGMR basiert primär auf Fällen zum englischen Recht. Da im englischen Strafverfahren in der Regel die Jury und nicht der Tatrichter das Urteil fällt, ist dort eine auf den Richter limitierte

---

[936] Für die Anwendung des § 244 III 2 StPO etwa *H. Müller,* Geheimhaltung, S. 80ff. Den Zweifelssatz favorisiert demgegenüber *Lüderssen,* FS für Klug, S. 538.

[937] Vgl. BGH NStZ 2004, S. 343f.

[938] Vgl. BGH NStZ-RR 2008, S. 350f; BGH NStZ-RR 2005, S. 209.

[939] Vgl. BGH NStZ 2001,S. 609; BGH NStZ-RR 2009, S. 90.

[940] Vgl. BGH NStZ 2004, S. 343f; BGH NStZ-RR 2005, S. 209; *Eisenberg,* Rn. 118.

[941] So BGH HRRS 2004, Nr. 200, S. 8f. Dieses letzte Argument ist jedoch weniger überzeugend. Zum einen ist diese Möglichkeit potentiell in jedem Prozess gegeben. Zum anderen ist es Aufgabe der Exekutive, sich zwischen dem Schutz der Sicherheitsinteressen und dem Strafverfolgungsinteresse zu entscheiden.

[942] So *Gaede,* StraFo 2004, S. 197; *Gaede,* StV 2006, S. 604.

[943] Vgl. *Gaede,* StraFo 2004, S. 196 m.w.N.

Einsichtnahme unbedenklich, während in Deutschland eine gerichtsinterne Prüfung als *in camera*-Verfahren unzulässig ist.

(δ) Einfluss nachträglicher Rechtsschutzmöglichkeiten

Auf einer letzten Ebene wird das deutsche Modell durch nachträgliche Rechtsschutzmöglichkeiten vervollständigt. Ergänzend zum allgemeinen Revisionsverfahren kann der Angeklagte speziell gegen die Sperrerklärung vorgehen.[944] Hierzu kann er noch während des Strafverfahrens etwa eine Anfechtungsklage nach den §§ 40ff VwGO vor den Verwaltungsgerichten erheben.[945] Die erforderliche Klagebefugnis ergibt sich aus dem Anspruch auf ein faires Verfahren, der bei einer rechtswidrigen Sperrung relevanter Beweismittel verletzt sein könnte.[946] Wird eine entsprechende Klage erhoben, kann das Strafgericht die Hauptverhandlung für die Dauer des Verwaltungsverfahrens aussetzen.[947] Während dieser Unterbrechung prüft das Verwaltungsgericht die Aufhebbarkeit der Sperrerklärung. Innerhalb dieses Hauptsachverfahrens unterliegen die gesperrten Akten allerdings den bereits im Strafverfahren geltend gemachten Geheimhaltungsgründen, sodass in Parallele zu § 96 StPO die Vorlage der Akten nach § 99 I 2 VwGO verweigert werden kann.

Im Gegensatz zum Strafverfahren kann die Vorlageverweigerung jedoch auf Antrag eines der Beteiligten in einem geheimen Zwischenverfahren auf ihre Rechtmäßigkeit untersucht werden.[948] Diese Rechtmäßigkeitskontrolle erfolgt nicht durch das Verwaltungsgericht der Hauptsache, sondern durch einen besonderen

---

[944] Zu den verschiedenen Revisionsgründen vgl. KK-*Nack,* § 96 Rn. 37; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 112ff. Denkbar sind die unzulässige Nutzung von Beweissurrogaten, eine defizitäre Beweiswürdigung sowie die Nichtberücksichtigung eines erreichbaren Beweismittels.

[945] Nach ü.A. ist der Rechtsweg zu den Verwaltungsgerichten eröffnet, vgl. BGH NJW 1998, S. 3577; BGHSt 44, 107; BVerwG NJW 1987, S. 202; KK-*Nack,* § 96 Rn. 34; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 106. Primär kommt eine Anfechtungsklage in Betracht, vgl. *Kornblum,* S. 179. Zur Statthaftigkeit einer Verpflichtungsklage VG Weimar NVwZ-RR 2002, S. 394f.

[946] Vgl. Radtke/Hohmann-*Joecks,* § 96 Rn. 20; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 109. Für eine dem Angeklagten vorbehaltene Klagemöglichkeit vgl. *Kramer,* NJW 1984, S. 1506; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 106. Das angeführte Argument eines unzulässigen In-Sich-Prozesses greift aber zumindest bei verschiedenen Körperschaften auf Bundes- und Landesebene nicht. Für eine zusätzliche Klagebefugnis der Staatsanwaltschaft Krekeler/Löffelmann-*Löffelmann,* § 96 Rn. 10.

[947] Ein solcher Anspruch besteht nicht, wenn die Klage keine Erfolgsaussichten hat oder wenn das rechtsstaatliche Gebot der Verfahrensbeschleunigung das Aufklärungsinteresse überwiegt; vgl. allgemein zu dieser Möglichkeit BGH NStZ 1985, S. 466, 468; BGH NJW 2007, S. 3010, 3012; Krekeler/Löffelmann-*Löffelmann,* § 96 Rn. 10.

[948] Vgl. § 99 II 1, 3 VwGO. Der erforderliche Antrag ist beim Gericht der Hauptsache zu stellen, welches diesen Antrag weiterleitet; vgl. *Droste,* Handbuch, S. 593; *Gärditz/Orth,* JuS 2010, S. 319f; *Kornblum,* S. 175.

Fachsenat am Oberverwaltungsgericht beziehungsweise am Bundesverwaltungsgericht.[949] In diesem Zwischenverfahren ist die oberste Dienstbehörde verpflichtet die bis dahin gesperrten Akten vorzulegen.[950] Um den Geheimschutzinteressen der Exekutive gerecht zu werden, ist dieses Zwischenverfahren als ein *in camera*-Verfahren ausgestaltet.[951] Die geheimhaltungsbedürftigen Informationen werden daher ausschließlich dem Gericht vorlegt, welches unter Ausschluss der sonstigen Verfahrensbeteiligten über die Vorlagepflicht und damit der Geheimhaltungsbedürftigkeit der gesperrten Akten entscheidet.[952] Der Fachsenat fällt seine Entscheidung in einem Beschlussverfahren, das heißt ohne mündliche Verhandlung. Diese Entscheidung bindet zugleich das Gericht der Hauptsache. Steht der Zugang zu entscheidungserheblichen Erkenntnissen infrage, ist mit der Entscheidung über die Geheimhaltungsbedürftigkeit zugleich die Entscheidung im Hauptsacheverfahren vorgegeben.[953] Bei Bejahung der Geheimhaltungsbedürftigkeit wird daher das Verwaltungsgericht die Rechtmäßigkeit der Sperrerklärung annehmen und die Klage abweisen. Wird die Geheimhaltungsbedürftigkeit verneint, ist der Kläger in seinen Rechten verletzt und die Sperrerklärung ist nach § 113 I 1 VwGO aufzuheben. Im letztgenannten Fall muss die oberste Dienstbehörde erneut über eine Vorlage und den Erlass einer Sperrerklärung entscheiden.[954] Bei dieser Entscheidung kann sie allerdings auch wieder zur Abgabe einer gegebenenfalls besser begründeten Sperrerklärung kommen.[955] Wird umgekehrt auf den erneuten Erlass einer Sperrerklärung verzichtet, ist die Behörde zur Aktenvorlage an das Gericht der Hauptsache verpflichtet.[956] Die ehemals gesperrten Beweismittel können dann im Strafverfahren genutzt werden. Eine solche Offenlegungsentscheidung ist bei nachrichtendienstlichen Erkenntnissen jedoch relativ unwahrscheinlich, in den meisten Fällen erhalten die Gerichte aufgrund einer tatsächlichen oder vermeintlichen Geheimhal-

---

[949] Siehe § 99 II 4 i.V.m. § 189 VwGO; vgl. hierzu *Droste,* Handbuch, S. 593; *Gärditz/Orth,* JuS 2010, S. 319f; *Kornblum,* S. 175, sowie BT-Drs. 14/7474, S. 15. Bei Erkenntnissen des BfV, des BND und des MAD ist in der Regel das Bundesverwaltungsgericht zuständig, vgl. BT-Drs. 14/7474, S. 15; *Kornblum,* S. 176. Für den BND ergibt sich dies bereits § 99 II 2 i.V.m. § 50 I Nr. 4 VwGO.

[950] Siehe § 99 II 5 VwGO. Verweigert die Behörde dennoch die Vorlage, stellt das Gericht nach den Grundsätzen der Beweisverteilung die Rechtswidrigkeit der Vorlageverweigerung fest, vgl. *Gärditz/Orth,* JuS 2010, S. 320; BT-Drs. 14/6393, S. 11.

[951] Nach § 99 II 7–11 VwGO gelten die Regeln des materiellen Geheimschutzes.

[952] Aus besonderen Geheimhaltungsgründen kann die oberste Dienstbehörde verlangen, dass die Unterlagen nur in einer von ihr bestimmten Räumlichkeit zur Verfügung gestellt werden. Siehe § 99 II 8 VwGO.

[953] Vgl. *Droste,* Handbuch, S. 593; *Kornblum,* S. 175.

[954] Die ersetzende Entscheidung durch das Verwaltungsgericht ist wegen des Gewaltenteilungsgrundsatzes nicht möglich, es sei denn die Sperrung ist von vorneherein willkürlich.

[955] Vgl. BVerwG NVwZ 2010, S. 905, 910; VG Weimar, NVwZ-RR 2002, S. 394, 399.

[956] Eine direkte Übermittlung vom Fachsenat an das Gericht der Hauptsache findet aufgrund des damit verbundenen Risikos demgegenüber gerade nicht statt.

tungsbedürftigkeit die ergangene Sperrerklärung aufrecht.[957] Die kompensatorische Wirkung dieses nachträglichen Rechtsschutzes hängt damit maßgeblich davon ab, inwiefern die Gerichte die Geheimhaltungsinteressen des Staates mit den Rechtsschutzinteressen des Betroffenen in einen angemessenen Ausgleich bringen können.

Die bei einer staatlichen Geheimhaltung bestehenden verwaltungsgerichtlichen Rechtsschutzmöglichkeiten verteilen sich damit auf drei Ebenen. Auf der ersten Ebene steht das Strafverfahren, für welches die infrage stehenden Beweismittel gesperrt werden. Dieses Strafverfahren wird auf einer zweiten Ebene durch die verwaltungsgerichtliche Anfechtung der Sperrerklärung unterbrochen. Auf einer dritten Ebene folgt, bei einer erneuten Vorlageverweigerung, das geheime Zwischenverfahren, in dem über die Geheimhaltungsbedürftigkeit der gesperrten Beweismittel entschieden wird. Dieser Umweg über das Verwaltungsverfahren ist den unterschiedlichen Beweislastregeln der Straf- und Verwaltungsgerichtsbarkeit geschuldet. Im Strafverfahren liegt die Beweislast aufgrund der Unschuldsvermutung grundsätzlich beim Staat. Die mit der Geheimhaltung verbundenen Unsicherheiten wirken sich nach dem Zweifelssatz theoretisch zugunsten des Angeklagten aus. Eine allein dem Richter gegenüber erfolgende Offenlegung des Beweismaterials würde allerdings die Rechtsposition des Betroffenen verschlechtern, da er sich bei belastenden Erkenntnissen nicht gegen die vorgebrachten Tatsachen wehren könnte.[958] Im Gegensatz dazu findet der Zweifelssatz im Verwaltungsverfahren keine Anwendung.[959] Zwar muss das Verwaltungsgericht den Sachverhalt ebenfalls aufklären, bei Unklarheiten trifft jedoch den Betroffenen eine objektive Beweislast, wonach er die für ihn vorteilhaften Tatsachen belegen muss. Der Betroffene müsste dementsprechend die für die Rechtswidrigkeit der Sperrerklärung sprechenden Tatsachen vorbringen, wozu er bei einer Sperrerklärung nur selten in der Lage sein wird.[960] Ohne das verwaltungsgerichtliche *in camera*-Verfahren hätte er keine Chance auf Berücksichtigung der gesperrten Unterlagen. Anders als im Strafverfahren verbessert die auf den Fachsenat begrenzte Einsicht die im Verwaltungsverfahren bestehenden Rechtsschutzmöglichkeiten.[961] Die auf den Richter limitierten Offenlegungsmöglichkeiten können die Erfolgschancen seines Vorbringens nur verbessern, jedoch nicht verschlechtern.

---

[957] Allerdings existieren durchaus Fälle, in denen eine Sperrerklärung auch in Bezug auf Akten der Nachrichtendienste aufgehoben wurde. Dies geschah etwa in dem 2010 vor dem Bundesverwaltungsgericht verhandelten Verfahren um die Sperrung der *Eichmann*-Akten des Bundesnachrichtendienstes; vgl. hierzu den Beschluss des BVerwG vom 19.4.2010 – 20 F 13/09, NVwZ 2010, S. 905, sowie *Schnabel,* NVwZ 2010, S. 881ff.

[958] Vgl. BGH NJW 2000, S. 1661ff; BVerfG NJW 2000, S. 1175, 1178.

[959] Im Verwaltungsverfahren bestimmt sich die Beweislastverteilung allein nach den Regeln des materiellen Rechts, die sog. materielle Beweislast, vgl. *Gusy,* Grundrechte, S. 116, 117; Bader/Ronellenfitsch-*Heßhaus,* § 24 Rn. 15ff; *Margedant,* NVwZ 2001, S. 762.

[960] Zu den entsprechenden Nachteilen siehe *Droste,* Handbuch, S. 595.

[961] Vgl. BVerfG NJW 2000, S. 1175; BGH NJW 2000, S. 1661ff.

b) Während der Hauptverhandlung

Im Strafverfahren entscheiden die Strafgerichte grundsätzlich unabhängig vom Einfluss anderer staatlicher Organe über die Heranziehung von relevantem Beweismaterial.[962] Nach Art. 35 I GG sind insofern alle Behörden des Bundes und der Länder zur Rechts- und Amtshilfe verpflichtet. Dementsprechend muss dem gerichtlichen Ersuchen um Aktenvorlage oder Auskunft in aller Regel entsprochen werden. Eine Geheimhaltung relevanter Tatsachen ist als Eingriff in die Wahrheitsfindung nur unter strengen Voraussetzungen und bei Vorliegen überragend wichtiger Gemein- oder Individualgüter gestattet.[963] Eine solche Ausnahmekonstellation wurde vom Gesetzgeber in der bereits besprochenen Vorschrift des § 96 StPO vorgesehen. Die auf der Grundlage einer Sperrerklärung erfolgende Geheimhaltungsentscheidung wird zwar im Vorfeld einer Hauptverhandlung getroffen, hat jedoch unmittelbare Auswirkungen auf die Beweisaufnahme in der Hauptverhandlung. Die Sperrerklärung verhindert, dass die Erkenntnisse Inhalt der Akten werden oder auf sonstige Weise den Staatsanwaltschaften oder dem Gericht zur Verfügung stehen. Es gelten insofern die beschriebenen Rechtsfolgen. Das Gericht ist dementsprechend verpflichtet den unvollständigen Sachverhalt mit Hilfe von Beweissurrogaten weiter aufzuklären. Die staatliche Einflussnahme auf die Beweisgrundlage ist durch die Herabstufung des Beweiswerts beziehungsweise eine vorsichtige Beweiswürdigung unter Berücksichtigung des Zweifelssatz zu kompensieren. In den erwähnten Fällen kann zudem die Berücksichtigung eines hypothetischen Beweisergebnisses erforderlich sein. Insofern handelt es sich um die bereits beschriebene Situation der Sperrerklärung.[964]

Abgesehen von dieser anerkannten Geheimhaltungsentscheidung besteht die Möglichkeit, dass die Geheimhaltungsbedürftigkeit erst nach einer Übermittlung der Geheimdienstinformationen an die Staatsanwaltschaften deutlich wird. Diese Konstellation ist in zweierlei Hinsicht problematisch. Das erste Problem betrifft die Frage, ob bei einer Übermittlung die Zuständigkeit der sperrenden Stelle wechselt. Bejaht man dies, würde die oberste Dienstbehörde der Nachrichtendienste mit der Übermittlung an die Strafverfolgungsbehörden ihre Sperrbefugnis verlieren. Die Beantwortung dieser Frage entscheidet sich danach, ob es sich bei § 96 StPO um eine Regelung der Herausgabepflicht des § 95 StPO oder der Amtshilfepflicht des Art. 35 GG handelt. Im ersten Fall wäre die tatsächliche Sachherrschaft beziehungsweise der Gewahrsam maßgeblich, im zweiten Fall wäre auf die rechtliche Verfügungsmacht über die Akten abzustellen. Die an die rechtliche Verfügungs-

---

962 Vgl. *Droste,* Handbuch, S. 591; Radtke/Hohmann-*Kelnhofer,* § 244 Rn. 29. Das deutsche System sieht als objektives System dementsprechend gerade keine freie Verhandelbarkeit vor.

963 So auch die höchstrichterliche Rechtsprechung, vgl. etwa BGH NStZ 2005, S. 43; BGH NJW 1988, S. 2187f.

964 Vgl. Teil 2, IV.B.1.a)bb).

macht anknüpfende Ansicht hat den Vorteil, dass die Zuständigkeit nicht von einer gegebenenfalls zufälligen Gewahrsamsverschiebung abhängen würde und damit eine gewisse Kontinuität gewährleistet wäre. Bei genauerer Betrachtung ist die rechtliche Verfügungsmacht ebenfalls kein konstanter Faktor, da ihr Inhaber ebenso wie beim Gewahrsam je nach Sachverhalt wechseln kann.[965] Bei einer Übermittlung an die Strafverfolgungsbehörden wäre von einem solchen Wechsel der Verfügungsmacht spätestens mit Aufnahme der Geheimdienstinformationen in die staatsanwaltschaftlichen Ermittlungsakten auszugehen.[966] Im Gegensatz dazu führt die auf den Gewahrsam abstellende Auslegung bei Schriftstücken oder Aktenbestandteilen zu einer gewissen Transparenz, da sich dieser objektiv nach der allgemeinen Verkehrsanschauung beurteilt.[967] Für diese Ansicht sprechen zudem kompetenzrechtliche Erwägungen. Die Fachaufsichtsbehörde der übermittelnden Stelle kann einer Behörde keine verbindlichen Vorgaben machen, wenn diese nicht ihrer Fachaufsicht untersteht. Mit dem Wechsel des Gewahrsams wechselt folglich zugleich die Zuständigkeit für die Abgabe der Sperrerklärung. Es ist damit die oberste Dienstbehörde der jeweils die Akten verwahrenden Stelle zuständig. Die Dienste geben ihre Verantwortung mit der Übermittlung ab.[968] Sie können als außerhalb des Justizinnenraums stehende Stellen nicht mehr über die Akten verfügen.

Dieser Zuständigkeitswechsel wirft bei einer Übermittlung nachrichtendienstlicher Erkenntnisse zu Strafverfolgungszwecken die Anschlussfrage auf, ob Strafakten überhaupt tauglicher Gegenstand einer Sperrerklärung sein können. Rechtlich geht es darum, ob die Vorschrift des § 96 StPO die Pflicht zur Aktenvorlage nach § 199 II 2 StPO einschränken kann. Eine erste Ansicht bejaht die grundsätzliche Anwendbarkeit des § 96 StPO auf die Aktenvorlagepflicht der Staatsanwaltschaft.[969] Als Argument wird der ähnliche Wortlaut beider Vorschriften angeführt, die sich beide auf die „Vorlegung" von Akten beziehen.[970] Ob die Sperrerklärung allerdings ihre Wirkung entfaltet, bestimmt sich danach, ob das Gericht bereits von den zu sperrenden Erkenntnissen Kenntnis genommen hat oder nicht.[971] Die Aufnahme der Erkenntnisse in die Akten hindert eine Sperrerklärung nicht. Diese kann vielmehr bis zur inhaltlichen Kenntnisnahme der Akten durch das Gericht erfol-

---

965 Vgl. Löwe/Rosenberg-*Schäfer,* § 96 Rn. 34f.

966 Diese Einschätzung ergibt sich aus einer Parallele zu beigezogenen Akten. Für diese verbleibt die Zuständigkeit bei der Behörde, der die Akten sachlich zustehen, vgl. Löwe/Rosenberg-*Schäfer,* § 96 Rn. 99.

967 Vgl. hierzu Löwe/Rosenberg-*Schäfer,* § 96 Rn. 39.

968 Vgl. BGH NStZ 1996, S. 287f; BGHSt 18, 369f; *Gössel,* NStZ 1996, S. 288.

969 So Löwe/Rosenberg-*Schäfer,* § 96 Rn. 2, 99.

970 So Löwe/Rosenberg-*Schäfer,* § 96 Rn. 2.

971 Vgl. SK-StPO-*Wohlers,* § 96 Rn. 41. Zur Sperrerklärung nach Akteneingang vgl. *Meyer-Goßner*, § 96 Rn. 11. Ebenso *Eisenberg,* Rn. 2340, mit Verweis auf eine dementsprechende allgemeine Auffassung.

gen.[972] Spätestens ab dem Zeitpunkt der Hauptverhandlung wird auch nach dieser Ansicht eine Sperrerklärung nicht mehr für möglich gehalten.[973] Im Gegensatz dazu lehnt eine zweite Ansicht die Möglichkeit einer nachträglichen Sperrerklärung ab, sofern es sich um staatsanwaltschaftliche Strafakten eines anhängigen Strafverfahrens handelt.[974] Sobald die Strafverfolgungsbehörden das maßgebliche Beweismittel erlangt und in die Akten aufgenommen haben, seien die Schriftstücke nicht mehr fremd, sodass es bereits an einer Grundvoraussetzung des § 96 StPO fehlt.[975] Dieser Ansicht ist mit Blick auf die Gesetzessystematik zustimmen. Die Vorschrift des § 199 II 2 StPO widmet sich ausdrücklich dem Verhältnis zwischen Staatsanwaltschaft und Gericht und geht damit dem § 96 StPO vor.[976] Für geheimdienstliche Erkenntnisse kann eine Sperrerklärung damit (nur) solange abgegeben werden, wie diese noch nicht Akteninhalt geworden sind. Dies gilt allerdings nur für Aktenbestandteile. Weiterhin möglich ist die „Sperrung" geheimdienstlicher Ermittlungspersonen, da diese nicht „persönlich" in die Akte eingehen können. Ein Personalbeweis kann anders als ein Schriftstück nicht zur Aufnahme in eine Akte „übermittelt" werden. Da über das Zeugenwissen nur die jeweilige Person verfügt, ist deren übergeordnete Dienstbehörde weiterhin für die Sperrung zuständig. Bei einem geheimdienstlichen VE kann die Sperrerklärung dementsprechend weiterhin durch den Dienstvorgesetzten im Nachrichtendienstsektor abgegeben werden. Bei dokumentierten Vernehmungsprotokollen geht mit dem Gewahrsamswechsel demgegenüber zugleich ein Zuständigkeitswechsel einher.

c) Zwischenergebnis

Die Geheimhaltungsstrategie einer vollständigen Abschottung wird maßgeblich mit dem Mittel der Sperrerklärung verfolgt. Die in diesem Zusammenhang zu durchlaufenden Prozesse sind komplex. Die maßgeblichen Vorgänge spielen sich in einer Dreieckskonstellation zwischen dem Gericht beziehungsweise der Staatsanwaltschaft, den Nachrichtendiensten und der obersten Dienstbehörde ab (Abb. 4). Die Durchführung des Strafverfahrens ist trotz der durch die Sperrerklärung ver-

---

[972] So *Eisenberg,* Rn. 2340; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 82; SK-StPO-*Wohlers,* § 96 Rn. 41.

[973] So *Eisenberg,* Rn. 2340.

[974] Vgl. BGHSt 18, 369f; OLG Hamburg StV 1984, S. 11f; vgl. auch Radtke/Hohmann-*Joecks,* § 96 Rn. 10; KK-*Laufhütte,* § 147 Rn. 13; Graf-*Ritzert,* § 96 Rn. 1; SK-StPO-*Wohlers,* § 96 Rn. 11. Diese Rechtsprechung verkennt Löwe/Rosenberg-*Schäfer,* § 96 Rn. 2, wenn er von „einer in der Literatur vertretenen Ansicht" spricht.

[975] Allerdings widersprechen sich Vertreter dieser Ansicht zum Teil selbst. So schließt SK-StPO-*Wohlers,* § 96 Rn. 11, Ermittlungsakten der Staatsanwaltschaft aus dem Anwendungsbereich des § 96 StPO ausdrücklich aus. Dreißig Randnummern später (Rn. 41) erkennt er jedoch eine Rückgabepflicht von Akten an, die sich bereits in den Händen der Strafverfolgungsorgane befinden.

[976] Vgl. OLG Hamburg StV 1984, S. 11f.

kürzten Beweisgrundlage möglich. Voraussetzung ist allerdings, dass die Geheimhaltung nicht die Verfahrensfairness insgesamt gefährdet. Die besonderen Möglichkeiten der Beweiswürdigung und des Zweifelssatzes werden nach der Rechtsprechung als ausreichende Kompensationsmechanismen betrachtet.

2. Strategie der Richterbeteiligung

Die zweite Geheimhaltungsstrategie erfasst Fälle, in denen die Offenlegung ausschließlich gegenüber dem Richter erfolgt, während auf Verteidigungsseite weder der Beschuldigte beziehungsweise Angeklagte noch sein Verteidiger Zugang zu den geheimhaltungsbedürftigen Informationen erhalten.

a) Vor der Hauptverhandlung

Das Ermittlungsverfahren unterliegt grundsätzlich der Geheimhaltung.[977] Aufgrund der besonderen Relevanz dieses Verfahrensabschnitts für die spätere Hauptverhandlung enthält die Strafprozessordnung jedoch vereinzelte Beteiligungsrechte, die eine effektive Verteidigung gewährleisten sollen. In diesem Sinne soll bereits frühzeitig auf die Wahrung der Beschuldigtenrechte und die Justizförmigkeit des Verfahrens hingewirkt werden können.[978] Die Beteiligungsrechte sind im Vorverfahren recht schwach ausgeprägt, sodass der Beschuldigte und sein Verteidiger unter erleichterten Bedingungen ausgeschlossen werden können. Aus Gründen der Vollständigkeit werden die in diesem Zusammenhang bestehenden Ausschlussmöglichkeiten am Beispiel heimlicher Ermittlungsmaßnahmen und der richterlichen Vernehmung verdeutlicht.

aa) Heimliche Ermittlungsmaßnahmen

Werden nachrichtendienstliche Erkenntnisse als Spurenansatz herangezogen, kann die Anordnung einer heimlichen Ermittlungsmaßnahme durch den Richter erforderlich sein. Zwar ist der Beschuldigte nach § 137 I 1 StPO befugt sich in jeder Lage des Verfahrens, das heißt bereits im Ermittlungsverfahren, des Beistands eines Verteidigers zu bedienen.[979] Grundvoraussetzung für eine solche Hinzuziehung ist die Kenntnis von einem laufenden Ermittlungsverfahren, woran es bei heimlichen Ermittlungsmaßnahmen letztlich fehlt. Nach § 163a I 1 StPO ist der Beschuldigte zwar spätestens vor dem Abschluss der Ermittlungen zu vernehmen,

---

977 Vgl. *Roxin/Schünemann,* § 19 Rn. 64; § 39 Rn. 29.

978 Vgl. *Meyer-Goßner*, Vor § 137 Rn. 1.

979 Vgl. stellvertretend *Burhoff,* Rn. 1900.

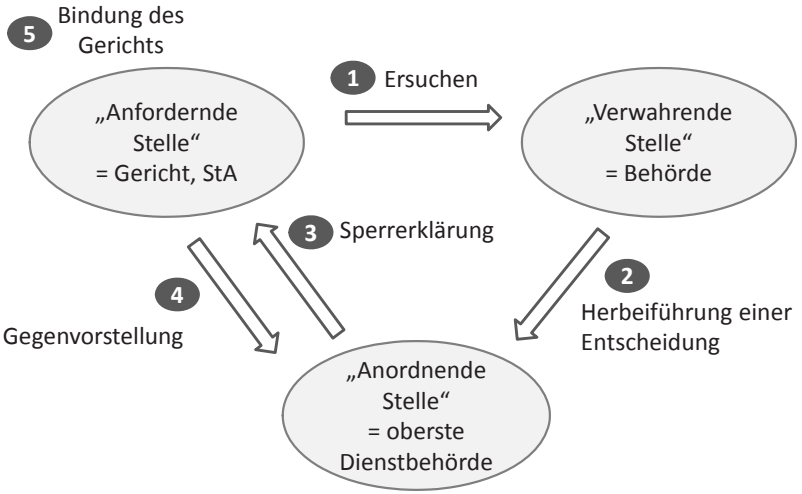

Abbildung 4: Dreiecksverhältnis bei einer Sperrerklärung im deutschen Recht

eine dem vorgelagerte Unterrichtungspflicht besteht aber nicht.[980] Die Staatsanwaltschaft kann die Vernehmung daher aus taktischen Gründen bis zu diesem letztmöglichen Zeitpunkt hinauszögern. Diese Abschottungsstrategie kann in bestimmten Fällen notwendig sein, da heimliche Ermittlungsmaßnahmen bei einem vorab informierten Beschuldigten in aller Regel überflüssig wären. In diesen Fällen erlangt der Beschuldigte erst mit der Vernehmung Kenntnis von der Überwachung. Erst ab diesem Zeitpunkt kann er einen Verteidiger bestellen, sodass weite Teile des Ermittlungsverfahrens ohne den Beschuldigten und seinen Verteidiger ablaufen können.

Trotz der gesetzlichen Anerkennung heimlicher Ermittlungsmaßnahmen kann die damit einhergehende Geheimhaltung bedenklich sein. Die Heimlichkeit der Ermittlungsmaßnahmen ist oftmals mit einem für den Beschuldigten nachteiligen Informationsvorsprung zugunsten der Strafverfolgungsbehörden verbunden. Das Informationsgefälle sowie die Verhältnismäßigkeit der Maßnahme insgesamt sollen dabei unter anderem durch die Existenz präventiver Kontrollmechanismen kompensiert werden. Die Betrachtung der tatsächlichen Verhältnisse macht jedoch deutlich, dass der Richtervorbehalt diesen Anforderungen oftmals nicht gerecht wird.[981] Zwar hat das Bundesverfassungsgericht[982] jüngst konkrete Vorgaben zur

---

980 Vgl. *Heghmanns,* FS für Eisenberg, S. 518.

981 Vgl. zur Ausgleichsfunktion und zur Kritik Teil 2, III.B.5.c)dd).

Stärkung des Richtervorbehalts aufgestellt, inwiefern diese Forderungen die bisherigen Defizite beheben können, bleibt jedoch abzuwarten. Eine Kompensation durch eine spätere Offenlegung im Hauptverfahren ist häufig nicht ausreichend. Die im Ermittlungsverfahren getroffenen Entscheidungen können die späteren Verfahrensvorgänge oftmals erheblich beeinflussen, ohne dass eine spätere Korrektur möglich ist.[983] Dem Ermittlungsverfahren kommt entgegen seiner ursprünglichen Konzeption längst keine bloß vorbereitende Funktion mehr zu. Werden beispielsweise entlastende Erkenntnisse nicht als solche erkannt, ist dieses Defizit im Hauptverfahren oftmals nicht mehr behebbar.

bb) Richterliche Vernehmung nach § 168c StPO

Eine zweite Ausschlussmöglichkeit betrifft die richterliche Vernehmung nach § 168c StPO. Diese Variante ist sowohl für das Ermittlungs- als auch das Hauptverfahren von Belang. Wird beispielsweise eine Ermittlungsperson der Nachrichtendienste als Zeuge richterlich vernommen, können diese Erkenntnisse nach § 251 StPO über die Verlesung in die Hauptverhandlung eingeführt werden. Da hierdurch faktisch ein Teil der Hauptverhandlung vorweggenommen wird, normiert § 168c II StPO als Regel ein Anwesenheitsrecht der Staatsanwaltschaft, der Verteidigung und des Beschuldigten.[984] Nach § 168c III 1 StPO kann jedoch die Anwesenheit des Beschuldigten ausgeschlossen werden, wenn diese den Untersuchungszweck gefährdet. Zweck der Untersuchung ist eine möglichst vollumfassende und unverfälschte Sachverhaltsaufklärung.[985] Diese kann bei einer Sperrerklärung gefährdet sein, wenn die oberste Dienstbehörde einer richterlichen Vernehmung des Zeugen nur unter Ausschluss des Beschuldigten zustimmt.[986] Eine solche Ausschlussmöglichkeit ist in Bezug auf den Verteidiger nicht vorgesehen. Obwohl der Verteidiger damit rein rechtlich zur Anwesenheit berechtigt ist, kann seine Beteiligung dennoch verhindert werden, indem er nicht benachrichtigt wird. . Die grundsätzlich nach § 168c V 1 StPO bestehende Benachrichtigungspflicht kann beispielsweise bei einer Gefährdung des Untersuchungserfolges nach § 168c V 2 StPO

---

982 Vgl. den Beschluss vom 11.6.2010 – 2 BvR 1046/08 = SVR 2010, S. 432f, in dem das Gericht strikte Einzelfallprüfung, ausreichende Begründungen sowie die Existenz eines richterlichen Eildienstes fordert.

983 Vgl. *Kühne,* Strafprozessrecht, Rn. 314.1.

984 So *Zacharias,* S. 196f. Bei einer staatsanwaltschaftlichen Zeugenvernehmung nach § 161a StPO steht weder dem Verteidiger noch dem Beschuldigten ein Anwesenheitsrecht zu. Dies ergibt sich bereits aus einem Umkehrschluss zu § 168c I StPO bzw. § 163a III 2 StPO. Die Vorschrift des § 161a StPO nimmt weder direkt noch über eine Verweisung auf deren Anwesenheit Bezug; vgl. *Burhoff,* Rn. 1876; KK-*Griesbaum,* § 161a Rn. 6; SK-StPO-*Wohlers,* § 161a Rn. 24; *Zacharias,* S. 196.

985 So *Zacharias,* S. 198.

986 Vgl. *Zacharias,* S. 198.

entfallen. Dem Begriff des Untersuchungserfolgs liegt ein engeres Verständnis zugrunde als dem des Untersuchungszwecks. Der „Untersuchungserfolg" ist in diesem Fall der Erhalt einer wahrheitsgemäßen, später verwertbaren Zeugenaussage.[987] Trotzdem kann der Untersuchungserfolg ebenfalls durch eine Sperrerklärung gefährdet sein und damit das Entfallen der Benachrichtigungspflicht rechtfertigen.[988] Wird eine solche Erfolgsgefährdung bejaht, ist der Verteidiger zwar weiterhin zur Teilnahme berechtigt, faktisch wird er dieses Recht mangels Kenntnis nicht wahrnehmen können.[989] Die Annahme einer Gefährdung liegt im Ermessen des vernehmenden Richters. Hierbei ist zu berücksichtigen, dass das bloße Vorliegen der Sperrerklärung das Gericht nicht von der Prüfung der konkreten Gefährdungsvoraussetzungen des § 168c V 2 StPO entbindet.[990] Die Nichtbeachtung dieser Vorgabe kann ein Verwertungsverbot begründen.[991] Im Ergebnis wird dem Verteidiger damit zwar ein uneinschränkbares Anwesenheitsrecht bei einer richterlichen Vernehmung zugestanden, dieses Recht kann jedoch durch einen Benachrichtigungsverzicht umgangen werden. In diesem Fall findet die richterliche Vernehmung ohne den Beschuldigten und seinen Verteidiger statt, sodass auf die protokollierten Wahrnehmungen des Richters zurückgegriffen werden muss. Da die gesetzlich vorgesehenen Beteiligungsrechte des Verteidigers entgegen der Grundregel entfallen, bedarf diese Vorschrift einer restriktiven Auslegung.[992] Ergänzend muss der Tatrichter die hierdurch bedingte Einschränkung des Fragerechts bei der Beweiswürdigung berücksichtigen.[993]

cc) Zwischenergebnis

Diese beiden Beispiele verdeutlichen, dass die Anwesenheits- und Akteneinsichtsrechte der Verteidigung vor der eigentlichen Hauptverhandlung relativ schwach ausgebildet sind. Zwar wurde keine der dargestellten Ausschlussmöglichkeiten ausdrücklich zum Schutz nationaler Sicherheitsinteressen vorgesehen, dennoch können diese Mechanismen zum Geheimnisschutz herangezogen werden. Wird allerdings die Hauptverhandlung durch bestimmte Vorgänge im Ermittlungsverfahren vorgezeichnet, kann zumindest der Verteidiger rechtlich nicht an der Beteiligung gehindert werden. Faktische Ausschlussmöglichkeiten sind weiterhin denkbar. Diese bieten jedoch nur einen geringen Geheimnisschutz, sodass dieser

---

987 Vgl. KK-*Griesbaum,* § 168c Rn. 17; *Freyschmidt/Ignor,* NStZ 2004, S. 467.

988 Inwiefern eine Vertraulichkeitszusage einen derartigen Verzicht gestattet, ist unklar, vgl. Löwe/Rosenberg-*Schäfer,* § 96 Rn. 65.

989 Vgl. hierzu *Roxin/Schünemann,* § 19 Rn. 64; § 39 Rn. 33.

990 Vgl. BGH NJW 2003, S. 3142 sowie *Meyer-Goßner*, § 168c Rn. 5.

991 Vgl. *Meyer-Goßner*, § 168c Rn. 6.

992 Vgl. *Tiedemann/Sieber,* NJW 1984, S. 749. Ebenso BGH NStZ 1984, S. 36, 39.

993 Vgl. BGH NJW 1980, S. 464f, sowie *Zacharias,* S. 201.

Strategie in Bezug auf die Nutzung von Geheimdienstinformationen keine allzu hohe Relevanz zukommt.

b) Verbot des in camera-Verfahrens in der Hauptverhandlung

Die Teilnahme des Verteidigers an der Hauptverhandlung wird durch die Strafprozessordnung umfassend garantiert. Eine auf das Gericht der Hauptsache beschränkte Offenlegung unter Ausschluss des Angeklagten ist grundsätzlich unzulässig. Die Rechtsprechung lehnt ein strafprozessuales *in camera*-Verfahren und damit eine einseitige Akteneinsicht durch das Gericht „in der Kammer" ausdrücklich ab.[994] Inhaltlich ist dieses Verbot unter anderem der Notwendigkeit effektiver Verteidigungsmöglichkeiten geschuldet, die ausgehend vom Anspruch auf rechtliches Gehör und dem Grundsatz eines fairen Verfahrens die Kenntnis der maßgeblichen Beweismittel erforderlich machen.[995] Der gerichtlichen Entscheidung dürfen letztlich nur solche Tatsachen zugrunde gelegt werden, über die der Angeklagte sachgemäß unterrichtet wurde und zu denen er Stellung nehmen konnte.[996] Eine sperrbedingte Geheimhaltung nachrichtendienstlicher Erkenntnisse erfasst damit nicht allein die Einsichtnahme durch die Verteidigung, sondern zugleich das Gericht.[997] Sofern der Richter damit Zugang zu bestimmten Erkenntnissen hat, sind diese umgekehrt auch der Verteidigung zugänglich zu machen.[998] Eine etwaige Vertraulichkeitszusage der Ermittlungsbehörde oder die Einstufung einer Akte als Verschlusssache entfaltet für das Gericht keine Bindungswirkung.[999]

In der Strafprozessordnung existieren keine Vorschriften, die den Ausschluss des Verteidigers aus der Hauptverhandlung aus Gründen der nationalen Sicherheit gestatten.[1000] Dieser ist vielmehr während der gesamten Hauptverhandlung zur Anwesenheit berechtigt.[1001] Eine Missachtung dieser Vorgaben begründet einen absoluten Revisionsgrund nach § 338 Nr. 5 StPO. Im geheimdienstrelevanten Bereich

---

994 Vgl. BGH NStZ 2000, S. 265f; BGH NJW 2000, S. 1661ff sowie BVerfG NStZ-RR 2008, S. 16, für die Beschwerdeinstanz. Ebenso KK-*Nack,* § 96 Rn. 25. Anders als im Verwaltungsprozess liegt im Strafprozess die Beweislast aufgrund der Unschuldsvermutung beim Staat, sodass ein *in camera*-Verfahren die Rechtsposition des Angeklagten verschlechtern würde, vgl. *Gusy,* Grundrechte, S. 116 Fn. 108.

995 Vgl. BVerfG NJW 1990, S. 1104; Epping/Hillgruber-*Radtke/Hagemeier,* Art. 103 Rn. 8f; *Schlegel,* HRRS 2004, S. 411; Widmaier-*Schlothauer,* § 3 Rn. 37.

996 Vgl. BVerfG NJW 1994, S. 3219f.

997 Vgl. BGH NStZ 1997, S. 43f; SK-StPO-*Wohlers,* § 147 Rn. 46f; *Zacharias,* S. 289.

998 BVerfG NStZ-RR 2008, S. 16f. Sämtliche Beweismittel sind dem Angeklagten und dem Richter daher in gleicher Art und Weise zugänglich zu machen.

999 Vgl. Widmaier-*Eschelbach,* § 28 Rn. 22.

1000 Vgl. BGH NJW 2000, S. 1661; BVerfG 1 BvR 385/90 Abs. Nr. 93, 94; BVerfG NStZ-RR 2008, S. 16f; BVerfG NJW 2006, S. 1048f.

1001 Vgl. *Roxin/Schünemann,* § 44 Rn. 40.

kommt lediglich ein Ausschluss nach § 138a II StPO in Betracht, wenn in Bezug auf den Verteidiger der Verdacht einer Straftat nach § 129a StGB besteht.[1002] Eine solche Ausschließung erfasst das gesamte Verfahren und soll den Mandanten vor belastenden Aussagen seines eigenen Verteidigers schützen. Da ein Ausschluss nach § 138 StPO damit lediglich bei Interessenskonflikten mit der Verteidigungsrolle und nicht zum Schutz nationaler Sicherheitsinteressen besteht, kann diese Geheimhaltungsvariante vorliegend außer Betracht bleiben.[1003]

Im Übrigen sind zeitlich limitierte Ausschlussmöglichkeiten grundsätzlich nicht vorgesehen. Denkbar ist lediglich ein faktischer Ausschluss des Verteidigers. Eine entsprechende Möglichkeit bietet die kommissarische Vernehmung nach § 223 StPO, die eine Zeugenvernehmung durch einen ersuchten beziehungsweise beauftragten Richter außerhalb der Hauptverhandlung gestattet.[1004] Im geheimdienstrelevanten Bereich kommt eine kommissarische Vernehmung in Betracht, wenn ein Zeuge aufgrund einer Sperrerklärung für eine persönliche Vernehmung nicht zur Verfügung steht.[1005] Die richterliche Vernehmung kann damit letztlich Beweise für die Hauptverhandlung sichern.[1006] Werden die in diesem Kontext verfassten Niederschriften unter den Voraussetzungen des § 251 II StPO in der Hauptverhandlung verlesen, wird diese hierdurch zumindest teilweise vorweggenommen.[1007] Die grundsätzlich fortbestehenden Anwesenheitsrechte können für den Angeklagten rechtlich nach § 247 StPO und für den Verteidiger faktisch nach § 224 I 2 StPO ausgeschlossen werden.[1008] Das für den Verteidiger grundsätzlich umfassende Anwesenheitsrecht kann wie bereits im Rahmen des § 168c StPO nach § 224 I 2 StPO durch einen Verzicht auf eine Benachrichtigung umgegangen werden.[1009] Abgese-

---

[1002] Weitere Ausschließungsmöglichkeiten sind das strafbare Zusammenwirken mit dem Mandanten. Vgl. insgesamt zu § 138a StPO *Roxin/Schünemann,* § 19 Rn. 48ff.

[1003] Interessant wäre wiederum der Fall, in dem sowohl nationale Sicherheitsinteressen als auch eine Konstellation des § 138 StPO zusammentreffen.

[1004] Sie kann sowohl im Eröffnungs- als auch im Hauptverfahren zur Anwendung kommen, vgl. KK-*Gmel,* § 223 Rn. 2; *Meyer-Goßner*, § 223 Rn. 10.

[1005] Vgl. *Meyer-Goßner*, § 223 Rn. 6. Bei der Sperrerklärung handelt es sich um ein anders nicht zu beseitigendes Hindernis.

[1006] Zu dieser Funktion vgl. KK-*Gmel,* § 223 Rn. 1.

[1007] Vgl. Graf-*Ritscher,* § 223 Rn. 1; KK-*Gmel,* § 223 Rn. 1; *Meyer-Goßner*, § 223 Rn. 1; *Roxin/Schünemann,* § 44 Rn. 10. Allerdings entscheidet das Gericht der Hauptsache über die Verlesbarkeit, vgl. BGHSt 33, 70, 75; *Meyer-Goßner*, § 223 Rn. 1; *Tiedemann/Sieber,* NJW 1984, S. 762. Selbst der BGH betont, dass die kommissarische Vernehmung „ihrem Wesen nach gleichsam einen Teil der Hauptverhandlung" bildet, so BGHSt 9, 24, 27.

[1008] Zum Ausschluss des Angeklagten *Meyer-Goßner*, § 223 Rn. 20. Vgl. zur Verteidigerbeteiligung KK-*Gmel,* § 224 Rn. 3. Nach § 224 I 1 StPO entfällt lediglich die Anwesenheitspflicht, vgl. BGH NJW 1984, 247; *Tiedemann/Sieber,* NJW 1984, S. 758. Der Verteidiger kann selbst bei einer Gefährdung des Zeugen nicht ausgeschlossen werden, vgl. BGHSt 32, 115, 129; BGH NStZ 1984, S. 36, 39; *Meyer-Goßner*, § 223 Rn. 19f; Löwe/Rosenberg-*Schäfer,* § 96 Rn. 71; *Tiedemann/Sieber,* NJW 1984, S. 759.

[1009] Ebenfalls in diese Richtung *Wattenberg,* StV, S. 695.

hen von dieser Sonderkonstellation finden sich in der Strafprozessordnung indes keine Vorschriften, die einen Verteidigerausschluss unter Verweis auf nationale Sicherheitsinteressen erlauben.

Letztlich ist es nach wie vor unzulässig, Geheimdienstinformationen in der Hauptverhandlung nur dem Richter offenzulegen und der Angeklagtenpartei vorzuenthalten. Der Angeklagte hat im Prozess daher grundsätzlich denselben Informationsstand wie der Tatrichter.[1010]

3. Strategie der Verteidigerbeteiligung

Nach einer dritten Geheimhaltungsstrategie wird allein der Beschuldigte beziehungsweise Angeklagte ausgeschlossen. Diese Variante war zum Teil bereits Gegenstand der vorangegangenen Ausführungen und soll daher lediglich um ein paar zusätzliche Aspekte ergänzt werden.

a) Vor der Hauptverhandlung

Das Ermittlungsverfahren ist grundsätzlich geheim, sodass die Beteiligungsrechte des Beschuldigten deutlich schwächer ausgebildet sind als im öffentlichen Hauptverfahren. Wie bereits im Zusammenhang mit der Strategie der Richterbeteiligung angedeutet, darf die richterliche Vernehmung nach § 168c III 1 StPO unter Ausschluss des Beschuldigten erfolgen. Anders als im Rahmen der Hauptverhandlung ist der Ausschluss des Beschuldigten nach § 168c StPO gerade nicht als Ausnahme, sondern als Regelfall konzipiert. Gefährdet die Anwesenheit des Beschuldigten den Untersuchungszweck, kann dies einen Ausschluss rechtfertigen. Eine solche Gefährdung ist beispielsweise anzunehmen, wenn die oberste Dienstbehörde der Nachrichtendienste die richterliche Vernehmung vom Ausschluss des Beschuldigten abhängig macht.[1011] Da eine Missachtung dieser Forderung üblicherweise zu einer vollständigen Sperrung des Zeugen führt, kann die Anwesenheit des Beschuldigten bei einer Nutzung von Geheimdienstinformationen eine vollumfassende und unverfälschte Sachverhaltsaufklärung und damit den Zweck der Untersuchung i.S.d. § 168c III 1 StPO gefährden.[1012] Die Abwägung des staatlichen Aufklärungsinteresses gegen die Verteidigungsbelange des Beschuldigten wird im Stadium des Ermittlungsverfahrens daher regelmäßig zugunsten des Aufklärungsinteresses ausfallen.[1013] Eine solche Geheimhaltungsstrategie ist hinsichtlich ihrer Auswirkungen

---

[1010] Dieser Ansatz wirkt sich bei einer Zurückhaltung entlastenden Beweismaterials nicht zwingend zugunsten des Angeklagten aus, da eine Kompensation lediglich über das Modell der Beweissurrogation und der vorsichtigen Beweiswürdigung möglich ist.

[1011] Vgl. *Zacharias,* S. 198.

[1012] Vgl. *Zacharias,* S. 198.

[1013] Vgl. *Zacharias,* S. 199.

auf das Strafverfahren in aller Regel unbedenklich, da das Teilnahmerecht des Verteidigers weiterhin besteht. Zudem wird der Angeklagte spätestens in der Hauptverhandlung über den Inhalt der Vernehmung in Kenntnis gesetzt.[1014] In Bezug auf eventuell betroffene nationale Sicherheitsinteressen bietet diese Möglichkeit allerdings nur einen bedingten Geheimnisschutz, da der zu schützende Zeuge über die Beteiligung und Wahrnehmung des Verteidigers identifizierbar wird.[1015]

Darüber hinaus kann ein Ausschluss des Beschuldigten auf einer Absprache mit dem Verteidiger beruhen, wofür dieser im Gegenzug beispielsweise Einsicht in geheimhaltungsbedürftige Akten erhalten kann.[1016] Eine solche Absprache ist jedoch nur auf freiwilliger Basis möglich.[1017] Die staatlichen Geheimschutzinteressen können dadurch nur bedingt gewahrt werden, weil der Verteidiger bei einer Missachtung seines Versprechens keine Sanktionen befürchten muss und die Geheimhaltung allein von seiner Kooperationsbereitschaft abhängig ist. Derartige Vereinbarungen bieten den Geheimdiensten mangels bindender Wirkung kaum einen ausreichenden Geheimnisschutz. Zudem können sie die Vertrauensbasis zwischen dem Verteidiger und seinem Mandanten belasten.[1018] Inwiefern eine solche Absprache in der Praxis tatsächlich genutzt wird, hängt davon ab, ob die damit verbundenen Belastungen für das Mandantschaftsverhältnis durch die Vorteile einer frühzeitigen Akteneinsicht aufgewogen werden.[1019]

b) Während der Hauptverhandlung

Während der Hauptverhandlung wird dem Angeklagten im Grundsatz eine ununterbrochene Anwesenheit gewährleistet.[1020] Seine Beteiligung soll eine effektive Wahrnehmung der Verteidigungsrechte ermöglichen und zur Wahrheitsermittlung beitragen.[1021] Grundlage dieser Gewährleistung sind unter anderem der Anspruch auf rechtliches Gehör, der *fair trial*-Grundsatz und das Verteidigungsrecht aus Art. 6 III lit. c EMRK.[1022] Auf einfachgesetzlicher Ebene stellt die Vorschrift des

---

1014 Vgl. *Zacharias,* S. 198.

1015 Vgl. *Zacharias,* S. 200f, wonach in besonders gravierenden Fällen die richterliche Fürsorgepflicht einen Verzicht auf die Aussage gebietet.

1016 Zu dieser Möglichkeit *Zacharias,* S. 208f. Kritisch *E. Müller,* NJW 1981, S. 1806.

1017 Vgl. *Zacharias,* S. 208.

1018 So *Zacharias,* S. 208f.

1019 Insofern kritisch *E. Müller,* NJW 1981, S. 1806.

1020 So der Beschluss des BGH vom 21.4.2010, GSSt 1/09, sowie *Bung,* HRRS 2010, S. 50; Widmaier-*Krause,* § 7 Rn. 14. Zur Unverzichtbarkeit des Anwesenheitsrechts BGH NJW 1976, S. 1108.

1021 Vgl. BGHSt 3, 187, 190; BGHSt 3, 384, 386; *Bung,* HRRS 2010, S. 50; KK-*Gmel,* § 230 Rn. 1.

1022 So *Schlegel,* HRRS 2004, S. 411; *Zacharias,* S. 229. Nach Art. 14 III lit. d IPBPR kommt diesem Anspruch sogar der Charakter eines Menschenrechts zu, vgl. *Bung,* HRRS 2010, S. 50.

§ 230 I StPO sicher, dass eine Hauptverhandlung gegen einen ausgebliebenen Angeklagten nicht stattfindet.[1023] Die Missachtung dieser Vorgabe begründet nach § 338 Nr. 5 StPO ebenfalls einen absoluten Revisionsgrund.[1024] Der Präsenz des Angeklagten kommt damit ein hoher Stellenwert zu, sodass sein Ausschluss nur in bestimmten Ausnahmefällen und lediglich vorübergehend möglich ist.[1025]

Eine ausdrücklich auf den Schutz nationaler Sicherheitsinteressen ausgerichtete Ausnahmeregelung existiert nicht. In streng limitierten Ausnahmefällen kommt allerdings eine Anwendung des § 247 StPO in Betracht. Nach dieser Vorschrift kann der Angeklagte von einer Zeugenvernehmung sowie einer Vernehmung nach § 247a StPO entfernt werden.[1026] In formeller Hinsicht bedarf die Ausschließung nach § 247 StPO eines förmlichen Gerichtsbeschlusses, der nach vorheriger Anhörung i.S.d. § 33 I StPO nach § 35 I 1 StPO zu verkünden ist.[1027] Der Beschluss muss nach § 34 StPO begründet werden. Die Entscheidung selbst steht im pflichtgemäßen Ermessen des Gerichts.[1028] In materieller Hinsicht kann die Entfernung auf Aspekte der Wahrheitsgefährdung nach Satz 1 oder des Zeugenschutzes nach Satz 2 gestützt werden.[1029] Die erstgenannte Ausschließung im Interesse der Sachaufklärung bedarf einer hinreichend konkreten Gefahr für die Wahrheitsfindung im Einzelfall.[1030] Demgegenüber muss sich die zweitgenannte Ausschließung zumindest beim Schutz erwachsener Zeugen auf die dringende Gefahr eines schwerwiegenden Nachteils für die Gesundheit stützen können und durch konkrete Umstände begründet sein.[1031] Beide Varianten kommen bei einer Nutzung von Geheimdienstinformationen in Betracht. In Bezug auf den Zeugenschutz birgt beispielsweise die Identifizierung eines nachrichtendienstlichen Informanten oftmals erhebliche Risiken für die körperliche Integrität des Zeugen.[1032] In Bezug auf die Wahrheitsfindung kann eine drohende Sperrerklärung den Verlust eines Beweismittels begründen und damit eine Beeinträchtigung i.S.d. § 247 StPO darstellen.[1033] Eine

---

[1023] Diesem Anwesenheitsrecht korrespondiert in § 231 StPO eine Anwesenheitspflicht.

[1024] Aufgrund der revisionsrechtlichen Relevanz machen die Gerichte von dieser Möglichkeit nur selten Gebrauch, vgl. *Weigend,* DJT, C 53.

[1025] So BGH vom 21.4.2010, GSSt 1/09. Ebenso Julius-*Julius,* § 247 Rn. 1.

[1026] Vgl. BGH NStZ 2006, S. 648f; Julius-*Julius,* § 247 Rn. 1ff, 6; *Kornblum,* S. 178. Zu den sonstigen Ausnahmen von der Anwesenheitspflicht siehe *Pfeiffer* StPO, § 230 Rn. 1. Zum Ausnahmecharakter vgl. Widmaier-*Krause,* § 7 Rn. 33.

[1027] Vgl. BGH NStZ 2002, S. 44; Julius-*Julius,* § 247 Rn. 7; Widmaier-*Krause,* § 7 Rn. 36. Nicht ausreichend ist eine Verfügung des Vorsitzenden, vgl. *Meyer-Goßner*, § 247 Rn. 14.

[1028] Zum Charakter als Ermessensentscheidung vgl. Julius-*Julius,* § 247 Rn. 6. Zur Begrenzung auf ein Auswahlermessen vgl. Graf-*Berg,* § 247 Rn. 9.

[1029] Vgl. Julius-*Julius,* § 247 Rn. 2ff; *Meyer-Goßner*, § 247 Rn. 3.

[1030] Vgl. Graf-*Berg,* § 247 Rn. 4f; KK-*Diemer,* § 247 Rn. 5.

[1031] Vgl. Graf-*Berg,* § 247 Rn. 5; KK-*Diemer,* § 247 Rn. 11.

[1032] Zur Anwendbarkeit auf Informanten und VE vgl. Julius-*Julius,* § 247 Rn. 5.

[1033] Vgl. KK-*Diemer,* § 247 Rn. 5.

Entfernung des Angeklagten ist damit aus den in § 96 StPO anerkannten Gründen möglich.[1034] Im Anschluss an die Vernehmung ist der Angeklagte wieder zur Hauptverhandlung zuzulassen. Nach § 247 Satz 4 StPO muss er über den Inhalt des Gesagten unterrichtet werden. Diese Unterrichtung erstreckt sich auf den „wesentlichen Inhalt" der getätigten Aussagen. Dies soll sicherstellen, dass der Angeklagte über den gleichen Wissensstand verfügt wie die sonstigen Verfahrensbeteiligten.[1035] Über die Wesentlichkeit entscheidet der Vorsitzende nach pflichtgemäßem Ermessen.[1036] Da die Angaben zur Person nicht zwingend zu diesen wesentlichen Angaben zählen, kann die Identität des Zeugen damit grundsätzlich gegenüber dem Angeklagten geheim gehalten werden.[1037]

Die Auswirkungen dieser Geheimhaltungsstrategie auf das Strafverfahren erscheinen zunächst erheblich, da der Angeklagte weder einen persönlichen Eindruck vom Aussageverhalten des Zeugen erhält noch dessen Glaubwürdigkeit durch unmittelbare Fragen testen kann. Diese Einschränkungen werden allerdings weitgehend kompensiert. So ist der Ausschluss auf dringende Ausnahmefälle und bestimmte Vernehmungssituationen beschränkt.[1038] Defizite in Bezug auf das Fragerecht können zum Teil durch die Vorlegung eines Fragenkatalogs an den Zeugen behoben werden.[1039] Zudem ist der Angeklagte unverzüglich nach der Vernehmung über den Inhalt des Gesagten zu unterrichten.[1040] Diese Unterrichtung muss sämtliche für eine effektive Verteidigung erforderliche Informationen enthalten, sodass dem Angeklagten letztlich nur der unmittelbare Eindruck, nicht jedoch das zur Verteidigung erforderliche Sachwissen vorenthalten wird. Da der Verteidiger der Vernehmung allerdings weiterhin beiwohnen darf, werden die Nachrichtendienste aus Quellenschutzgründen in den meisten Fällen eine vollständige Sperrung des Zeugen favorisieren.

Im Ergebnis kann der Angeklagte in wenigen Ausnahmefällen für eine kurze Zeitt von der Hauptverhandlung ausgeschlossen werden. Diese Geheimhaltung darf sich jedoch nicht auf inhaltliche Aspekte beziehen, die vor den übrigen Beteiligten erörtert wurden. Eine Anwendung des § 247 StPO auf sonstige Vorgänge mit

---

[1034] Vgl. BGH NStZ 1996, S. 648; *Meyer-Goßner*, § 247 Rn. 4; *Soiné,* NStZ 2007, S. 251; *Zacharias,* S. 230.

[1035] Vgl. Julius-*Julius,* § 247 Rn. 10.

[1036] Vgl. *Meyer-Goßner*, § 247 Rn. 16.

[1037] So KK-*Senge,* Vor § 48 Rn. 13. Die Reichweite dieser nachträglichen Unterrichtung unterliegt dem pflichtgemäßen Ermessen des Gerichts.

[1038] Vgl. zum Ausnahmecharakter BT-Drs. 10/6124, S. 14; *Zacharias,* S. 236. Siehe zum Äußerungsrecht § 257 I StPO.

[1039] Vgl. hierzu § 240 II StPO; vgl. BGH NStZ 2001, S. 212, 216; BGH NStZ 1993, S. 292; BGH NStZ-RR 2002, S. 176; *Meyer-Goßner*, § 247 Rn. 18.

[1040] Vgl. BGH NStZ 1983, S. 181; BT-Drs. 10/6124, S. 13f; Widmaier-*Krause,* § 7 Rn. 37; *Meyer-Goßner*, § 247 Rn. 16.

eigenständiger verfahrensrechtlicher Bedeutung ist nicht möglich.[1041] Der Ausschließung des Angeklagten nach § 247 StPO kommt daher ein absoluter Ausnahmecharakter zu.[1042] Sein Verteidiger ist zudem weiterhin anwesend.

4. Strategie des Geschworenenausschlusses

Dem deutschen Strafprozessrecht liegt kein Geschworenensystem zugrunde, sodass diese Geheimhaltungsstrategie im deutschen Recht nicht in Betracht kommt.

5. Strategie des Öffentlichkeitsausschlusses

Die letzte Geheimhaltungsstrategie betrifft den Ausschluss der Öffentlichkeit. Im Ermittlungsverfahren ergibt er sich bereits aus der geheimen Konzeption des Ermittlungsverfahrens, welches im Gegensatz zum Hauptverfahren von vorneherein als nichtöffentliches Verfahren ausgestaltet ist.[1043]

a) Voraussetzungen einer Geheimhaltung

Die Hauptverhandlung unterliegt demgegenüber dem Öffentlichkeitsgrundsatz, der als prägendes Prinzip des rechtsstaatlichen Verfahrens durch verschiedene Vorschriften gewährleistet wird.[1044] Nach § 169 GVG ist die strafrechtliche Hauptverhandlung vom Aufruf der Sache nach § 243 I 1 StPO bis zur Verkündung der Urteile und Beschlüsse öffentlich.[1045] Die Verletzung dieser Vorgabe begründet einen absoluten Revisionsgrund nach § 338 Nr. 6 StPO. Allerdings wird die Öffentlichkeit selbst im Rahmen der Hauptverhandlung nicht uneingeschränkt gewährleistet. Das Gericht ist unter den Voraussetzungen der §§ 170ff GVG berechtigt die Öffentlichkeit durch Beschluss von bestimmten Verfahrensabschnitten auszuschließen.[1046] Im Bereich der nationalen Sicherheitsinteressen sind vor allem die Ausschlussgründe nach § 172 Nr. 1 und Nr. 1a GVG von Interesse. Diese gestatten den Ausschluss der Öffentlichkeit, wenn eine Gefährdung der Staatssicherheit

---

[1041] Vgl. Julius-*Julius,* § 247 Rn. 8; Widmaier-*Krause,* § 7 Rn. 33. Dementsprechend scheidet eine Anwendung des § 247 StPO für eine Augenscheinseinnahme (BGH NStZ 2001, S. 262), die Verhandlung über die Vereidigung des Zeugen (BGH NStZ 1999, S. 522) und die Verlesung von Urkunden (BGH NStZ 1997, S. 402) aus. Vertiefend zu Umfang und Dauer des Ausschlusses vgl. KK-*Diemer,* § 247 Rn. 6ff; Julius-*Julius,* § 247 Rn. 8ff.

[1042] Vgl. Julius-*Julius,* § 247 Rn. 1.

[1043] So stellvertretend *Roxin/Schünemann,* § 16 Rn. 2; § 39 Rn. 29; *Zacharias,* S. 195.

[1044] So BGHSt 9, 280f; 21, 72f, sowie KK-*Diemer,* § 169 GVG Rn. 1.

[1045] Vgl. Graf-*Allgayer,* § 169 GVG Rn. 2. Auf konventionsrechtlicher Ebene findet sich der Öffentlichkeitsgrundsatz in Art. 6 I 1, 2 1. Halbsatz EMRK.

[1046] Daneben finden sich in Nr. 131ff RiStBV Hinweise, wann der Ausschluss der Öffentlichkeit geboten sein kann, vgl. Widmaier-*Krause,* § 7 Rn. 42.

(Nr. 1) oder eine Gefährdung des Lebens, des Leibes oder der Freiheit eines Zeugen oder einer anderen Person zu besorgen ist (Nr. 1a). Ausreichend ist die bloße Besorgnis einer Gefährdung, ein Schaden wird nicht gefordert.[1047] Sind diese Voraussetzungen erfüllt, entscheidet das Gericht nach seinem Ermessen über das Ob und die Dauer des Öffentlichkeitsausschlusses.[1048] Bei einer Nutzung von Geheimdienstinformationen wird sich dieses Ermessen regelmäßig auf einen Öffentlichkeitsausschluss reduzieren.[1049] Als Minus zu einer vollständigen Sperrerklärung werden die klassischen Sperrgründe regelmäßig einen Ausschluss der Öffentlichkeit rechtfertigen. Sofern nicht auch in Bezug auf die Urteilsverkündigung eine Ausschließung nach § 173 II i.V.m. den §§ 171b, 172 GVG für erforderlich gehalten wird, erfolgt diese nach § 173 I GVG wieder öffentlich.

b) Auswirkungen auf das Strafverfahren

Im Ermittlungsverfahren ist diese Geheimhaltungsstrategie kaum von Bedeutung, da es ohnehin weitgehend unter Ausschluss der Öffentlichkeit erfolgt und dem Informations- und Kontrollinteresse durch die folgende öffentliche Hauptverhandlung ausreichend Rechnung getragen werden kann. Die Hauptverhandlung muss grundsätzlich unter Beteiligung der Öffentlichkeit erfolgen. Dieses Öffentlichkeitsgebot kann bei einer Nutzung von Geheimdienstinformationen aufgrund bestehender Schutzinteressen nicht immer durchgehalten werden. Die Abwägungsentscheidung des Gerichts zugunsten eines Öffentlichkeitsausschlusses ist unter Verhältnismäßigkeitsgesichtspunkten jedoch zumindest dann nicht zu beanstanden, wenn hierdurch die Abgabe einer umfassenderen Sperrerklärung verhindert werden kann. In einer solchen Konstellation kommt dem gerichtlichen Aufklärungsinteresse und den Schutzinteressen des Zeugen beziehungsweise der Dienste ein höheres Gewicht zu als dem Kontroll- und Informationsinteresse der Öffentlichkeit.

V. Zusammenfassung zur deutschen Rechtslage

Die Nutzung von Geheimdienstinformationen im deutschen Strafprozess wurde anhand von zwei Einflussfaktoren untersucht: die deutsche Sicherheitsarchitektur und die staatlichen Geheimhaltungsinteressen. Als Hauptproduzent von Geheimdienstinformationen wurde dabei die klassische Trias aus BfV, BND und MAD zugrunde gelegt.

[1047] Vgl. *Zacharias,* S. 222.

[1048] Vgl. KK-*Diemer,* § 169 GVG Rn. 1.

[1049] Vgl. KK-*Diemer,* § 172 GVG Rn. 1.

In Bezug auf den ersten Untersuchungsschwerpunkt konnte der Einfluss der Sicherheitsarchitektur auf die Besonderheiten geheimdienstlicher Ermittlungen und die strafprozessuale Nutzung von Geheimdienstinformationen nachgewiesen werden. Diese Architektur wird in Deutschland vor allem durch die Vorgaben des Föderalismus und des Trennungsgebots bestimmt. Die Konzeption als staatliches Frühwarnsystem und die damit verbundene strategische und langfristige Vorfeldbeobachtung wird aufgrund der mit dem Trennungsgebot verbundenen Begrenzungen akzeptiert. Wegen dieser Strukturvorgaben sind die deutschen Nachrichtendienste – trotz erheblicher Annäherungstendenzen – weiterhin eine der wenigen staatlichen Behörden, die anlasslose, einzelfallunabhängige und flächendeckende Beobachtungsmaßnahmen durchführen können.

Kommt es zu einem Austausch mit dem Strafverfolgungssektor, droht allerdings eine Umgehung dieser Begrenzungen. Aus diesem Grund sieht das deutsche Recht spezielle Übermittlungs- und Verwertungsregeln vor, welche die Heranziehung von Geheimdienstinformationen limitieren. Eine Übermittlung zu Strafverfolgungszwecken ist danach nur bei schweren beziehungsweise staatschutzrelevanten Delikten möglich. Die strafprozessuale Verwertung wird über die Voraussetzungen des hypothetischen Ersatzeingriffs legitimiert.

Darüber hinaus wird der Einfluss der Sicherheitsarchitektur an den Auswirkungen einzelner Reformen des Sicherheitswesens deutlich. Mit der Aufweichung des Trennungsgebots nehmen zugleich die Überschneidungsbereiche zum Strafverfolgungs- und Polizeisektor zu. Diese betreffen etwa die jeweils anwendbaren Ermittlungsschwellen und -befugnisse.

In Bezug auf den zweiten Untersuchungsschwerpunkt wurde die unterschiedliche Bedeutung der einzelnen Geheimhaltungsstrategien deutlich. Sofern die Geheimdienstinformationen den Geheimdienstsektor überhaupt verlassen, gelten in den verschiedenen Phasen des Strafverfahrens unterschiedliche Schutzstandards. Im grundsätzlich geheimen Ermittlungsverfahren ist ein Ausschluss der Beteiligungsrechte unter erleichterten Bedingungen möglich. Sofern bereits in dieser Phase wesentliche Entscheidungen für das Hauptverfahren getroffen werden, ist die Verteidigung allerdings zur Teilnahme berechtigt.

Erreichen die Geheimdienstinformationen das Stadium der Hauptverhandlung, ist eine Geheimhaltung nur unter strengen Voraussetzungen möglich. Ausdrücklich unzulässig ist ein strafrechtliches *in camera*-Verfahren und damit eine in der Hauptverhandlung allein dem Richter vorbehaltene Kenntnisnahme. Ebenso wenig darf das Anwesenheitsrecht des Verteidigers während der Hauptverhandlung beschnitten werden. Weitgehend unproblematisch ist demgegenüber der zeitweise Ausschluss des Angeklagten von bestimmten Vernehmungssituationen. Abseits

dieser Ausnahmeregelungen darf beziehungsweise muss der Angeklagte während der gesamten Hauptverhandlung ununterbrochen anwesend sein.

Als zentrales Geheimhaltungsinstrument hat sich bei der Untersuchung allerdings die Abgabe einer Sperrerklärung nach § 96 StPO herauskristallisiert. Eine solche Sperrerklärung ermöglicht in besonderen Ausnahmefällen eine vollständige Abschottung geheimhaltungsbedürftiger Informationen. Die Durchführung des Strafverfahrens ist trotz der verkürzten Beweisgrundlage möglich. Als zentrale Ersatzstrategien sieht das deutsche Strafverfahren die Möglichkeit der Beweissurrogation und die Einwirkungsmöglichkeiten des Richters durch die vorsichtige Beweiswürdigung vor. Verglichen mit der vollständigen Abschottung mittels einer Sperrerklärung spielen die sonstigen Geheimhaltungsstrategien in geheimdienstrelevanten Sachverhalten nur eine untergeordnete Rolle.

Insgesamt wird dem Strafrichter damit eine herausragende Stellung zugesprochen. Er soll über die Institute des hypothetischen Ersatzeingriffs und der Beweissurrogation einerseits sowie über eine vorsichtige Beweiswürdigung andererseits die Umgehung strafprozessualer Garantien verhindern. Die Verantwortung für ein faires Strafverfahren auf der Grundlage geheimdienstlich gewonnener Erkenntnisse trägt damit primär das zur Entscheidung berufene strafrichterliche Entscheidungsgremium. Erst wenn dieses Gremium an seine Grenzen gelangt, erfolgt eine Verfahrenseinstellung beziehungsweise eine Verlagerung der Verantwortung in ein verwaltungsgerichtliches *in camera*-Verfahren.

Teil 3

Nutzung von Geheimdienstinformationen im amerikanischen Strafprozess

Die nachfolgenden Ausführungen behandeln die Nutzung von Geheimdienstinformationen im amerikanischen Strafprozess. Ebenso wie im deutschen Landesbericht werden die Grundlagen des Strafverfahrensrechts (I.), die Produzenten von Geheimdienstinformationen (II.), die Auswirkungen der Sicherheitsarchitektur auf die Informationsnutzung (III.) sowie der Einfluss nationaler Sicherheitsinteressen auf die Nutzung und Offenlegung von Geheimdienstinformationen behandelt (IV.).

I. Relevante Grundlagen des amerikanischen Strafprozessrechts

In Parallelität zum deutschen Landesbericht konzentriert sich die Darstellung auf die vorliegend relevanten Grundzüge des amerikanischen Strafprozessrechts. Es wird ein Überblick über die wesentlichen Rechtsquellen und Beweisregeln sowie die Zuständigkeiten bei geheimdienstrelevanten Strafsachen gegeben.

A. Rechtsquellen und Verfahrensablauf

Das amerikanische Strafverfahrensrecht wird erheblich durch verfassungsrechtliche Vorgaben geprägt. Die zentralen Verfahrensrechte sind in den ersten zehn Zusatzartikeln der *Bill of Rights* sowie der *due process*-Klausel des 14. Zusatzartikels enthalten.[1] Da die amerikanische Rechtsordnung zum *Common Law* gehört, kommt zudem dem gerichtlich geschaffenen Fallrecht ein erheblicher Einfluss zu.[2] Nach dem Konzept der *stare decisis* sind Urteile höherer Instanzen für nachrangige Gerichte bindend.[3] Auf horizontaler Ebene ist ein Gericht ebenfalls an seine vorhe-

---

[1] Vgl. *Becker,* RIDP/IRPL 2009, S. 344; *Hay,* S. 257; *Herrmann,* FS für Jescheck, S. 1298; *Rogall,* in: Wolter, S. 119.

[2] Vgl. hierzu insgesamt *Gehring,* S. 23ff; Kilian/Heussen-*Lejeune,* Kap. 12 Rn. 1ff; *Reinbacher,* S. 17ff.

[3] Vgl. *Reinbacher,* S. 19.

rigen Urteile gebunden, sofern nicht signifikante Unterschiede eine Abweichung rechtfertigen. Dieses *case law* wird fortlaufend durch geschriebenes Gesetzesrecht, das sogenannte *statutory law*, fixiert und ergänzt. Dieser Prozess hat im Laufe der Zeit zu einer weitgehenden Kodifikation des amerikanischen Strafprozessrechts geführt. Für Strafverfahren wurden im *18 Title* des *United States Codes,*[4] in den *Federal Rules of Criminal Procedure* (FRCrimP) und den *Federal Rules of Evidence* (FRE) einheitliche Regeln für das Verfahrens- und Beweisrecht auf Bundesebene geschaffen. Gleichwertig existieren daneben die Prozessordnungen der 50 Bundesstaaten sowie diejenige des *District of Columbia*. Diese lehnen sich weitgehend an die Mindeststandards der *Bill of Rights* und der Bundesregelungen an.[5] Aufgrund dieser Angleichung vermitteln die Regeln des Bundesstrafprozesses eine Art Grundkonsens der im amerikanischen Strafverfahrensrecht geltenden Grundstrukturen. Die Nutzung von Geheimdienstinformationen kann daher maßgeblich an den Vorgaben der Verfassung sowie den bundesrechtlichen Regelungen der FRCrimP und der FRE dargestellt werden. Für die Militärkommission werden die zentralen Regelungen im *Military Commission Act 2009* (MCA 2009) und dem *Manual for Military Commissions 2010* festgehalten.[6] Der MCA 2009 regelt die Befugnis zur Errichtung von Militärkommissionen und definiert die relevanten Straftaten, Beschuldigtenrechte und Verfahrensregeln. Das *Manual for Military Commissions 2010* wird vom Verteidigungsministerium erlassen und enthält die anwendbaren Verfahrens- und Beweisregeln. Daneben existieren spezielle *Military Commission Rules of Evidence*. Inhaltlich orientieren sich diese Sonderregelungen stark an den Vorschriften der zivilen Bundesgerichtsbarkeit, sodass auf etwaige Besonderheiten nur bei eventuellen Abweichungen hingewiesen wird.[7]

In Bezug auf den konkreten Verfahrensablauf unterscheidet der amerikanische Strafprozess mehrere Abschnitte.[8] Maßgeblicher Auslöser für das Greifen der Verfahrensregeln ist die Festnahme des Verdächtigen. Diese erfordert eine durch hinreichende Gründe gestützte richterliche Anordnung.[9] Die amerikanischen Strafverfolgungsbehörden unterliegen dabei dem Opportunitätsprinzip. Bestätigt sich der Verdacht, wird nach *Rule* 3 FRCrimP eine erste Anklageschrift (die *complaint*)

---

[4] Die Arbeit orientiert sich dabei an der US-amerikanischen Schreibweise, die zunächst Title, Name des Gesetzes und dann den konkreten Paragraphen benennt. 18 U.S.C. widmet sich dem Bereich *Crimes and Criminal Procedure*.

[5] Vgl. hierzu *Krüßmann,* S. 167; *Perron,* Beweisantragsrecht, S. 454; *Trüg,* S. 34.

[6] Die aktuellen Regeln finden sich unter http://www.mc.mil/legalresources/MilitaryCommissionsDocuments/CurrentDocuments.aspx [Stand: 1.5.2012].

[7] Vgl. die allgemeine Übersicht zu den Unterschieden bei *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 38ff.

[8] Vertiefend zu den Verfahrensabschnitten *Krüßmann,* S. 197ff; *Trüg,* S. 38ff.

[9] Dieser sog. *warrant* muss sich auf einen *probable cause* stützen; vgl. *Hay,* Rn. 708. Insgesamt vertiefend *Krüßmann,* S. 197, 203; *Thaman,* in: Perron, S. 494; *Trüg,* S. 38.

verfasst.[10] In komplexen Delikten kann die Staatsanwaltschaft unterstützend eine sogenannte *investigative grand jury* einberufen.[11]

Im nächsten Verfahrensabschnitt erfolgt die Überprüfung des Anklagevorwurfs.[12] Diese kann als *preliminary hearing* oder als *grand jury review* ausgestaltet sein.[13] Das *preliminary hearing* findet vor dem Magistratsgericht unter Beteiligung des Angeschuldigten *(defendant)* statt. In diesem Verfahrensstadium werden die Anklage und das Vorliegen eines hinreichenden Tatverdachts unter Beteiligung der Staatsanwaltschaft und der Verteidigung einer gerichtlichen Prüfung unterzogen.[14] Im Bereich der schweren Delikte kann diese Überprüfung durch eine *grand jury review* erfolgen.[15] Diese wird durch den fünften Verfassungszusatz und die *Rule* 6 FRCrimP gewährleistet. Die aus ca. 20 Mitgliedern bestehende *grand jury* tagt geheim und überprüft *ex parte* und auf der Grundlage der von der Anklage vorgelegten Akten, ob für die Durchführung einer Hauptverhandlung hinreichende Anhaltspunkte vorliegen. Ein Richter ist nicht beteiligt, der *grand jury* selbst wird allerdings eine gerichtsähnliche Funktion zuerkannt.[16] Der Verfahrensabschnitt kann mit einer Bestätigung der Anklage, dem *indictment,* beendet werden.[17] Dieses bildet die formale Voraussetzung für den Übergang in das gerichtliche Hauptverfahren.

Das Hauptverfahren gliedert sich oftmals in die Abschnitte *arraignment*, *pretrial discovery* und *trial*. Das *arraignment* ist ein Anklageeröffnungsverfahren, in welchem dem Beschuldigten die Anklage übergeben und eine Stellungnahme ermöglicht wird.[18] Im *pleading* kann er sich für schuldig oder unschuldig erklären. Im *pretrial stage* können die Parteien durch entsprechende Anträge, die sogenannten *pretrial motions,* beim Tatrichter Fehler im Vorverfahren geltend machen.[19] In diesem Zusammenhang können sie Akteneinsicht beziehungsweise die Offenlegung relevanter Umstände sowie den Ausschluss unzulässiger Beweismittel bean-

---

[10] Vgl. *Trüg,* S. 39.

[11] Vgl. *Grunwald,* S. 254.

[12] Der Angeklagte kann auf dessen Durchführung nach Rule 5.1. (a)(1) FRCrimP allerdings verzichten, vgl. *Krüßmann,* S. 198f; *Trüg,* S. 41, 43.

[13] Vertiefend *Trüg,* S. 41f.

[14] Vgl. *Krüßmann,* S. 199; *Thaman,* in: Perron, S. 501. *Trüg,* S. 51, verweist darauf, dass der Richter des *preliminary hearing* in der Regel nicht mit dem Richter der späteren Hauptsache identisch ist.

[15] Vertiefend *Scheb/Scheb II,* S. 357f; *Trüg,* S. 42ff.

[16] Vgl. *Trüg,* S. 43.

[17] Nach *Thaman,* in: Perron, S. 534, können die bisherigen Verfahrensabschnitte als funktionales Äquivalent zum deutschen Ermittlungsverfahren gesehen werden.

[18] Vgl. Rule 10, 11, 12 FRCrimP. Vertiefend *Scheb/Scheb II,* S. 358f.

[19] Vgl. *Scheb/Scheb II,* S. 358, 360.

tragen.[20] Auf der Basis dieser Anträge muss das Gericht die Staatsanwaltschaft zur Offenlegung sämtlicher offenlegungstauglicher Erkenntnisse bewegen.[21] Da die Parteien in diesem Verfahrensstadium die Beweismittel der Gegenseite sichten können, wird es auch als *discovery period* oder *pre-trial discovery* bezeichnet.[22] Dieser Verfahrensabschnitt soll einerseits eine ausreichende Vorbereitung der Parteien auf das Hauptverfahren ermöglichen und Überraschungsmomente verhindern, andererseits dient diese Phase der Herstellung der Waffengleichheit zu den Strafverfolgungsbehörden, die anders als der Beschuldigte über umfassende Ermittlungsmöglichkeiten verfügen.[23] Der eigentliche *trial*-Abschnitt und damit das Hauptverfahren ist nach dem sechsten Zusatzartikel grundsätzlich als *jury*-Verfahren ausgestaltet.[24] Das Geschworenengremium der Hauptverhandlung besteht in der Regel aus zwölf Personen und wird daher als *petit jury* bezeichnet.[25] Dieses ist von der *grand jury* zu unterscheiden, welche ihrerseits zu Ermittlungen befugt ist. Anders als die geheim über die Anklage entscheidende *grand jury* urteilen die Geschworenen in einem öffentlichen Hauptverfahren über die Schuldfrage. Die Mitglieder können jeder Gesellschaftsschicht angehören. Aufgrund dieser gesellschaftlichen Durchmischung wird den Geschworenen ein großer Erfahrungsschatz in Bezug auf die Beurteilung der Glaubwürdigkeit von Zeugen zugesprochen.[26] Tatsächlich wird nur ein geringer Teil der Straftaten vor Geschworenen abgeurteilt.[27] Allerdings hat der Betroffene bei schwerwiegenden Straftaten, den sogenannten *felony offenses,* einen Anspruch auf ein Geschworenen-Verfahren.[28] Da die geheimdienstrelevanten Bereiche des Terrorismus und des Staatsschutzes überwiegend Delikte der schweren Kriminalität abdecken, wird die Hauptverhandlung, sofern es zu einer kommt, in der Regel vor Geschworenen stattfinden.[29] Der

---

[20] Eine Auflistung der vor dem Hauptverfahren erforderlichen Anträge findet sich in Rule 12(b)(3) FRCrimP; vgl. auch *Krüßmann,* S. 202; *Thompson/Nored/Worrall/ Hemmens,* S. 52ff; *Trüg,* S. 48.

[21] Vgl. *Thompson/Nored/Worrall/Hemmens,* S. 52.

[22] Vgl. *Thompson/Nored/Worrall/Hemmens,* S. 52; *Scheb/Scheb II,* S. 360.

[23] So *Trüg,* S. 330.

[24] Vgl. Rule 23(a) FRCrimP; *Trüg,* S. 57. Grundsätzlich ist auch die Entscheidung durch einen Einzelrichter möglich (z.B. *bench trials* und *plea bargains*). Für eine solche Abweichung müssen jedoch der Angeklagte und die Strafverfolgung einstimmig auf eine Beteiligung der Geschworenen verzichten; vgl. hierzu *Perron,* in: ders., S. 503 Fn. 66; *Turner/Schulhofer,* S. 14.

[25] Vgl. Rule 23(b)(1) FRCrimP. In manchen Staaten ist die Zahl geringer, ein Minimum von sechs Personen wird aber als notwendig erachtet, vgl. *Trüg,* S. 50.

[26] Vgl. *Feeney/Herrmann,* S. 427.

[27] Vertiefend bei *Thaman,* in: Perron, S. 496f. Die sog. *plea bargains* spielen in diesem Zusammenhang eine große Rolle.

[28] Vgl. *Trüg,* S. 38.

[29] Zur überwiegenden Zahl von Verhandlungen mit Geschworenen bei *felony cases* vor den Bundesgerichten vgl. *Thaman,* in: Perron, S. 502. Siehe zudem auf der Website der amerikanischen Bundesgerichte die aktuelle Statistik Table D-4, abrufbar unter www.

Angeklagte kann auf dieses Recht nur im Einvernehmen mit dem Gericht und der Staatsanwaltschaft verzichten.[30]

Der Verfahrensablauf vor einer Militärkommission ist derjenigen der zivilen Strafgerichtsbarkeit sehr ähnlich. Allerdings sind sämtliche gerichtlichen Funktionen mit Militärpersonal besetzt. Die Verhandlung erfolgt dementsprechend vor einem Militärjuristen beziehungsweise einem *senior military officer* als Vorsitzenden und Geschworenen, die dem Militär angehören.[31] Außer bei Verhängung der Todesstrafe ist für die Verurteilung durch die Geschworenen keine Einstimmigkeit erforderlich. Anders als in zivilen Bundesverfahren genügt eine bloße Zwei-Drittel-Mehrheit.[32]

B. Grundprinzipien und Grenzen der Beweisführung

Die Grundprinzipien und Grenzen der Beweisführung wurden vom *Supreme Court* maßgeblich anhand der Garantien des vierten, fünften und sechsten Zusatzartikels zur Bundesverfassung entwickelt.[33] Die daraus entstandenen Beweisregeln wurden mit Erlass der *Federal Rules of Evidence* (FRE) im Jahr 1975 weitgehend gesetzlich fixiert und greifen vor allem in den kontradiktorisch ausgestalteten Verfahrensabschnitten.[34] Nachfolgend werden lediglich die für die vorliegende Untersuchung relevanten Aspekte erläutert.[35]

Vor der Durchführung des Hauptverfahrens werden in der Regel die bereits beschriebenen *pretrial motions* gestellt. Neben einer Offenlegung kann in diesem Zusammenhang der Ausschluss unzulässiger Beweismittel beantragt werden. Entsprechend diesen Anträgen werden die Beweismittel vor einer Präsentation im Hauptverfahren daher einer Prüfung durch den Richter unterzogen.[36] Zwar obliegt im amerikanischen Strafprozess die Beweisaufnahme grundsätzlich den Parteien, jedoch entscheidet das Gericht vorab, welche Beweise tatsächlich in der Hauptver-

---

uscourts.gov/Statistics/StatisticalTablesForTheFederalJudiciary/December-2011.aspx [Stand: 6.4.2013]. Danach kam es im Jahr 2011 zu 205 *bench trials* und 2.057 *jury trials*.

30 Rule 23 (2) FRCrimP; vgl. *Hay,* Rn. 724; *Krüßmann,* S. 202.

31 Vgl. 10 U.S.C. §§ 948h–948m; *Stuckenberg,* JZ 2006, S. 1146. Die Geschworenen werden durch das *Office of the Convening Authority* ausgewählt.

32 Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 39.

33 Vgl. hierzu *Trüg,* S. 385.

34 Vgl. *Herrmann,* Reform, S. 159; *Farnsworth/Sheppard,* S. 126; *Krüßmann,* S. 176; *Perron,* in: ders., S. 564. Allerdings finden sich in den FRE zahlreiche Durchbrechungen dieser ehemals strikten Regeln, vgl. *Thaman,* in: Perron, S. 510f.

35 Vgl. stattdessen vertiefend *Signorelli,* S. 329ff; *Thompson/Nored/Worrall/Hemmens,* S. 111ff.

36 Vgl. *Krüßmann,* S. 202; *Rogall,* in: Wolter, S. 122; *Thompson/Nored/Worrall/Hemmens,* S. 52.

handlung präsentiert werden dürfen. Nur innerhalb dieses Rahmens können die Parteien bestimmen, welche Beweise sie zur Verfügung stellen und welche sie zurückhalten.[37] Die zugelassenen Beweismittel sollen in einer auf Waffengleichheit angelegten Auseinandersetzung präsentiert werden, deren Fairness der Richter durch seine Vorabprüfung sicherstellen soll.[38] Hierdurch wird bereits im Vorverfahren geklärt, welche Beweismittel den Geschworenen zur Wahrheitsfindung vorgetragen werden dürfen und welche nicht. Auf einer ersten Stufe prüft der Richter die *admissibility* und damit die Zulässigkeit des Beweismittels.[39] Wann im Einzelfall von einer Zulässigkeit auszugehen ist, wird in den FRE zum Teil ausdrücklich festgelegt und beispielsweise bei fehlender Relevanz des Beweismittels verneint.[40] Die zweite Stufe ist die *exclusion of evidence* und damit der Ausschluss grundsätzlich relevanter Beweismittel. Hier werden rechtswidrige und unglaubwürdige Beweise vor dem Hauptverfahren ausgefiltert. Um Rechtswidrigkeit geltend zu machen, muss der Beschuldigte ein Rechtsschutzbedürfnis beziehungsweise eine individuelle Betroffenheit von der Rechtswidrigkeit nachweisen *(standing)*.[41] Die Beweislast für den Nachweis eines Beweisverwertungsverbots liegt grundsätzlich beim Beschuldigten.[42]

Zentrale Beweisregeln des amerikanischen Beweisrechts sind die *best evidence rule* in *Rule* 1002 FRE und die *hearsay rule* in *Rule* 802 FRE. Die *best evidence rule* betrifft Urkunden und Augenscheinsobjekte. Diese müssen grundsätzlich im Original und damit der bestmöglichen Beweisqualität vorgelegt werden.[43] Die *hearsay rule* bezieht sich auf Zeugen und Sachverständige und erklärt den Beweis vom Hörensagen für unzulässig. Diese Beweisregeln haben ihre Ursache in der Ausgestaltung des amerikanischen Strafverfahrens als adversatorisch geprägtes Geschworenen-Modell. Demnach soll der Angeklagte ein Beweismittel durch seine unmittelbare Wahrnehmung und die Möglichkeiten des Kreuzverhörs auf seine Glaubwürdigkeit testen können.[44] Dies ist nur möglich, wenn ihm die originären Beweismittel vorgelegt werden. Darüber hinaus soll eine emotionale und unsachliche Beeinflussung der Geschworenen durch irrelevante, unzuverlässige, sekun-

---

[37] Vgl. *Eser,* FS für Jung, S. 176; *Schmitz,* S. 83f.

[38] Vgl. *Herrmann,* Reform, S. 167f.

[39] Siehe Rule 104 FRE.

[40] Siehe Rule 402 FRE. Die entsprechende Definition von relevantem Beweismaterial findet sich in Rule 401 FRE.

[41] Vgl. *Rogall,* in: Wolter, S. 135; *Trüg,* S. 405.

[42] Vgl. *Rogall,* in: Wolter, S. 136. Dies gilt nicht für die Frage der Freiwilligkeit. Als Beweismaß greift der *preponderance of evidence*-Standard.

[43] Vgl. *Scheb/Scheb II,* S. 329; *Thaman,* in: Perron, S. 509; *Thompson/Nored/Worrall/Hemmens,* S. 223.

[44] Vgl. *Feeney/Herrmann,* S. 397.

däre oder rechtswidrige Beweismittel verhindert werden.[45] Die Geschworenen werden insofern als besonders schutzbedürftig empfunden, da sie anders als ein ausgebildeter Richter nicht unbedingt zwischen dem Beweiswert primärer und sekundärer Beweismittel unterscheiden können.[46] Beide Regelungen können durch Ausnahmen durchbrochen werden.[47]

Einen weiteren Begründungsansatz für die Annahme eines Beweisausschlusses bildet der sogenannte Disziplinierungs- beziehungsweise Abschreckungsgedanke. Dieser Aspekt hat sich in der allgemein gültigen *exclusionary rule* niedergeschlagen und wurde primär anhand des vierten Verfassungszusatzes entwickelt.[48] Ursprünglich sollte die *exclusionary rule* zugleich eine weitergehende Verletzung der Verfassungsgarantien, insbesondere der Privatsphäre, verhindern und die Integrität des Strafverfahrens sicherstellen. Spätestens seit den 1960er Jahren hat jedoch der Disziplinierungsgedanke als Begründungsansatz an Bedeutung gewonnen.[49] Danach dürfen Beweismittel nicht verwertet werden, wenn sie von den Strafverfolgungsbehörden unter Verstoß gegen gesetzliche oder verfassungsrechtliche Vorgaben erlangt wurden.[50] Rechtswidriges Handeln der Ermittlungsbehörden führt danach zur Unverwertbarkeit des Beweismittels, wodurch den Ermittlungsbehörden jeglicher Anreiz zur Vornahme rechtswidriger Ermittlungshandlungen genommen werden soll.[51] Die Verletzung der Privatsphäre spielt bei der Frage der Verwertbarkeit daher keine Rolle mehr.[52] Nach dem herrschenden Verständnis ist die mit der rechtswidrigen Erhebung verbundene Verletzung mit dem Erhebungsprozess abgeschlossen, sodass eine nachträgliche Kompensation durch die Annahme eines Beweisverbots weder möglich noch erforderlich ist.[53] Wann konkret von einem Disziplinierungsbedarf auszugehen ist, entscheiden die Gerichte anhand einer Interessensabwägung zwischen dem Nutzen eines Beweisausschlusses und den daraus resultierenden Kosten für die Wahrheitsfindung.[54] Infolge dieser Kosten-Nutzen-Abwägung wurde ein Verwertungsverbot bei mangelnder Effektivität oder bei

---

[45] Vgl. *Krüßmann,* S. 202; *Trüg,* S. 49. Die Geschworenen erhalten dann keinen Zugriff.

[46] Vgl. *Farnsworth/Sheppard,* S. 123, 128; *Thompson/Nored/Worrall/Hemmens,* S. 28.

[47] Vgl. hierzu Rule 801–807 FRE, sowie *Perron,* in: ders., S. 571; *Thaman,* in: Perron, S. 509; *Trüg,* S. 344.

[48] Vgl. *Weeks v. United States*, 232 U.S. 383 (S. Ct. 1914). Mit *Mapp v. Ohio*, 367 U.S. 643 (S. Ct. 1961) erfolgt die Ausdehnung der Regel über den 14. Zusatzartikel auch auf die Bundesstaatenebene; vgl. zudem *King,* Int'l Legal Persp. (12) 2002, S. 209f.

[49] Vgl. *Herrmann,* FS für Jescheck, S. 1299f; *Rogall,* in: Wolter, S. 125; *Trüg,* S. 387.

[50] Vgl. *Hay,* Rn. 707; *Rogall,* in: Wolter, S. 121.

[51] Vgl. *Trüg,* S. 387f. Vertiefend *Oaks,* U. Chi. L. Rev. (37) 1970, S. 665ff; S*cheb/ Scheb II,* S. 348ff.

[52] Eine Berücksichtigung ist höchstens unter verfahrensethischen Gesichtspunkten möglich, vgl. *Rogall,* in: Wolter, S. 125.

[53] Vgl. hierzu *Herrmann,* FS für Jescheck, S. 1300; *Rogall,* in: Wolter, S. 120ff, 125.

[54] Vgl. *Trüg,* S. 389f.

geringfügigen Rechtsverletzungen verneint.[55] Die Notwendigkeit einer Disziplinierung wurde ebenfalls abgelehnt, wenn die Ermittlungspersonen gutgläubig von der Rechtmäßigkeit der Ermittlungsmaßnahme ausgegangen sind *(good-faith exception)*.[56]

Die Reichweite eines Beweisausschlusses wird ebenfalls vom Disziplinierungsgedanken bestimmt. Nach der *fruit of the poisonous tree*-Doktrin erstreckt sich die Unverwertbarkeit zusätzlich auf alle Erkenntnisse, die indirekt auf dem ursprünglichen, illegalen Beweismittel beruhen.[57] Durch die Annahme einer Fernwirkung soll eine Umgehung durch Rückgriff auf mittelbar erlangte Beweismittel verhindert werden.[58] Allerdings wird diese Grundregel ebenfalls durch zahlreiche Ausnahmen und einen engen Anwendungsbereich relativiert.[59]

Wurden die genannten Hürden überwunden, können die zugelassenen Beweismittel den Geschworenen der Hauptverhandlung präsentiert werden.[60] Der Richter agiert als unparteiischer Schiedsrichter, der die Geschworenen über Rechtsfragen und Widersprüche aufklärt.[61] Nach dem *beyond reasonable doubt*-Standard muss für eine Verurteilung die Verwirklichung des Straftatbestands ohne einen begründeten Zweifel nachgewiesen werden.[62] Aspekte, die wiederum die Schuld beziehungsweise die Strafbarkeit des Täters ausschließen, sind vom Angeklagten zu belegen. Hierzu genügt allerdings, wenn der Angeklagte nach dem *preponderance of the evidence*-Standard überwiegende Zweifel im Sinne einer bloß 51%igen Sicherheit wecken kann.[63]

Die dargestellten Grundsätze kommen in ähnlicher Form in den Militärkommissionen zum Tragen. Mit der Reform des MCA 2009 wurde eine weitgehende Angleichung an die klassischen Beweisregeln der zivilen Bundesstrafgerichtsbarkeit erreicht.[64] In bestimmten Bereichen blieben die Anforderungen an die Beweis-

---

[55] Vgl. *Trüg,* S. 389f; *Herrmann,* FS für Jescheck, S. 1301.

[56] Vgl. *United States v. Leon*, 468 U.S. 897, 916 (9th Cir. 1984). Darin heißt es: "the exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates"; vgl. ebenso *Rogall,* in: Wolter, S. 124.

[57] Vgl. *Herrmann,* FS für Jescheck, S. 1307; *Rogall,* in: Wolter, S. 132.

[58] Vgl. *Trüg,* S. 451.

[59] Vertiefend *Herrmann,* FS für Jescheck, S. 1307ff; *Rogall,* in: Wolter, S. 122ff; *Trüg,* S. 400ff, 451ff, 476. Beispiele sind hypothetische Ermittlungsverläufe. Zudem dürfen rechtswidrige Beweis zur Erschütterung der Glaubwürdigkeit eines Zeugen und im Rahmen der Strafzumessung herangezogen werden, vgl. *United States v. Havens*, 446 U.S. 620, 625 (S. Ct. 1980); *Herrmann,* FS für Jescheck, S. 1301; *Trüg,* S. 397.

[60] Vertiefend *Schmitz,* S. 83f.

[61] Vgl. *Eser,* FS für Jung, S. 176; *Farnsworth/Sheppard,* S. 123; *Schmitz,* S. 84; *Thaman,* in: Perron, Beweisantragsrecht, S. 308; *Trüg,* S. 56.

[62] Vgl. *Thaman*, in: Perron, S. 507; *Thompson/Nored/Worrall/Hemmens,* S. 63.

[63] Vgl. *Thompson/Nored/Worrall/Hemmens,* S. 65; *Trüg*, S. 52f.

[64] Ein Vergleich der verschiedenen Rechtssysteme findet sich von offizieller Seite unter http://www.mc.mil/aboutus/LegalSystemComparison.aspx [Stand: 1.5.2012] sowie *Kris,*

führung zum Teil jedoch abgesenkt, um den besonderen Bedürfnissen bei militärischen Konflikten Rechnung zu tragen. Die Nutzung von Hörensagenbeweisen wird beispielsweise nach 10 U.S.C. § 949a(b)(3)(D) weitaus großzügiger und flexibler gehandhabt. Es genügt, wenn der Militärrichter die Unerreichbarkeit des Zeugen feststellt und dem sekundären Beweis eine gewisse Zuverlässigkeit und Beweiskraft bescheinigt.[65] Ebenfalls eingeschränkt wird die Selbstbelastungsfreiheit. Für die Verwertbarkeit einer Aussage genügt es, dass die Gesamtumstände auf die Zuverlässigkeit und einen ausreichenden Beweiswert hinweisen und die Aussage freiwillig gemacht wurde.[66] Die sonst erforderliche Verlesung der *Miranda*-Rechte ist nicht notwendig.[67] Diese begründen im Normalfall den Anspruch des Verdächtigen, über seine Rechte aufgeklärt zu werden. Diese Rechte beinhalten im Einzelnen die Aufklärung über das Aussageverweigerungsrecht, die Möglichkeit, einen Rechtsanwalt oder einen vom Staat gestellten Rechtsbeistand heranzuziehen, sowie den Verweis darauf, dass das Gesagte vor Gericht gegen ihn verwendet werden kann.[68]

C. Zuständigkeiten bei geheimdienstrelevanten Straftaten

Im amerikanischen Rechtssystem kommt eine strafrechtliche Nutzung von Geheimdienstinformationen sowohl vor den klassischen Strafgerichten als auch den militärisch geprägten *Military Commissions* in Betracht.[69] Die zivilen Strafgerichte sind für die Strafverfolgung von US-Bürgern sowie bei Inhaftierungen im Inland zuständig.[70] Die Zuständigkeitsverteilung wird durch den föderativen Charakter des amerikanischen Systems bestimmt. Demnach finden sich Strafgerichte sowohl auf Bundesebene als auch auf Ebene der Einzelstaaten.[71] Trotz der Regel-

---

J. Nat'l Sec. L. & Pol'y (5) 2011, S. 33ff. Vor der Reform waren die Unterschiede weitaus größer.

[65] Vgl. 10 U.S.C. § 949a(b)(3) sowie Military Commission Rules of Evidence 801, 803. Vertiefend *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 46, der davon ausgeht, dass sich die gelockerten Standards durchaus auch zugunsten des Angeklagten auswirken können.

[66] Vgl. 10 U.S.C. § 949a(b)(3)(B), Military Commission Rule of Evidence 304.

[67] Vgl. *Doyle,* CRS 2013, S. 6f.

[68] Siehe *Miranda v. Arizona*, 384 U.S. 436 (S. Ct. 1966); vgl. zudem *Hay*, Rn. 713.

[69] Die klassischen Militärgerichte, die sog. *Court Martials,* bleiben vorliegend außer Betracht. Zum einen sind die Prozessregeln weitgehend mit denen der Bundesgerichtsbarkeit identisch, zum anderen sind sie auf Verstöße von Militärangehörigen gegen das Militärstrafrecht, d.h. den Uniform Code of Military Justice, 10 U.S.C. §§ 801–946, begrenzt; vgl. *Manget,* Stan. L. & Pol'y Rev. 2006, S. 426; *Scheb/Scheb II,* S. 377.

[70] Siehe 28 U.S.C. §§ 1251–1631; vgl. insgesamt *Thompson/Nored/Worrall/Hemmens,* S. 37.

[71] Vgl. zu den unterschiedlichen Instanzen *Trüg,* S. 36f.

zuständigkeit der Einzelstaaten kann der Kongress bei Straftaten von staatenübergreifender beziehungsweise internationaler Bedeutung die Gerichtshoheit auf den Bund übertragen.[72] Ein solches Bedürfnis besteht etwa, wenn die Behörden auf Staatenebene nicht über die erforderlichen Ermittlungsmöglichkeiten oder im Bereich der Bundesstraftaten nicht über die erforderliche Zuständigkeit verfügen.[73] Hiervon ist etwa in Fällen des internationalen Terrorismus auszugehen, zumal es sich bei terrorrelevanten Delikten üblicherweise um Bundesstraftaten handelt.[74] Der Aufbau der Bundesgerichtsbarkeit ist unter anderem in Art. 3 Sec. 1 US-Verfassung vorgegeben, weswegen diese Gerichte auch als *Article III courts* bezeichnet werden.

Daneben existieren die sogenannten *Military Commissions*. Die Sondergerichtsbarkeit der Militärkommissionen wurde vom damaligen US-Präsident George W. Bush im November 2001 als Reaktion auf die Terroranschläge von New York zur Aburteilung von Terroristen für Kriegsverbrechen eingeführt.[75] Grundlage waren die verfassungsrechtlichen *war powers* des Präsidenten als Oberstem Befehlshaber aus dem ersten und zweiten Verfassungsartikel sowie die Ermächtigung des Kongresses vom 18. September 2001 in der *Authorization to Use Military Force* (AUMF).[76] Der AUMF ermächtigte den Präsidenten zum Einsatz der notwendigen militärischen Mittel gegen die Verantwortlichen der Terroranschläge vom 11. September 2001.[77] Zudem wurden die Militärkommissionen im *Uniform Code of Military Justice* (UCMJ) anerkannt.[78] Die ursprünglichen Regelungen wurden durch *Military Commissions Act 2006* (MCA 2006) und 2009 (MCA 2009) ergänzt.[79] Die Zuständigkeit der Militärkommissionen hängt maßgeblich vom Status des Betroffenen ab. Dieser muss als *alien unprivileged enemy belligerent* ergriffen werden.[80] Das

---

[72] Vgl. zur Regelzuständigkeit *Rogall,* in: Wolter, S. 117; *Thompson/Nored/Worrall/Hemmens,* S. 41.

[73] Die Zuständigkeit fehlt u.a. bei bundesrelevanten Fragenstellungen. Dies sind sämtliche Fragen, die typischerweise einen Bezug zur Bundesregierung, Bundesverfassung oder allgemein föderale Fragen betreffen, vgl. *Markwordt Skehan,* S. 93.

[74] Vgl. *Eligon*. So etwa die 18 U.S.C. § 2332b. Die Bundesstaaten haben ebenfalls *anti-terrorism statutes* erlassen. Vgl. zu Zuständigkeitsfragen *Krüßmann,* S. 168.

[75] Siehe die Presidential Military Order "Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism" in Federal Register Vol. 66, No. 222 vom 13.11.2011; vgl. *Maggs*, S. 464. Historisch gesehen kamen die Militärkommissionen bereits während des Zweiten Weltkriegs zur Anwendung, vgl. *Ex Parte Quirin*, 317 U.S. 1 (1942). Vertiefend *Maggs*, S. 463; *Stuckenberg,* JZ 2006, S. 1145f. Weitere Informationen von offizieller Seite finden sich unter http://www.mc.mil/aboutus/MilitaryCommissions History.aspx [Stand: 1.5.2012].

[76] Pub. L. No. 107-40, 115 Stat. 224 vom 18.9.2001; vgl. hierzu *Vervaele,* EJCCL & CJ 2005, S. 203ff.

[77] Vgl. *Hay,* Rn. 711; *Maggs*, S. 464; *Stuckenberg,* JZ 2006, S. 1146.

[78] Vgl. hierzu 10 U.S.C. §§ 821, 836.

[79] Vgl. zum MCA 2009 die Regeln in 10 U.S.C. §§ 948a–950t.

[80] Vgl. 10 U.S.C. §§ 948a (6), (7).

Merkmal des *unprivileged enemy belligerent* erfüllt derjenige, der sich als Mitglied oder Unterstützer der Taliban, der *Al Quaida* oder sonst eines Zusammenschlusses in feindlichen Kampfhandlungen gegen die USA oder einer ihrer Verbündeten engagiert.[81] Durch den Verweis auf *alien* scheidet eine Aburteilung von US-Bürgern durch eine Militärkommission aus. Diese ist nur bei Ausländern möglich.[82] Da insbesondere im Bereich der geheimdienstlichen Auslandsaufklärung Erkenntnisse anfallen, die für die Aburteilung eines vermutlichen Terroristen vor einer Militärkommission nutzbar sind, ist diese Sondergerichtsbarkeit in den funktionalen Rechtsvergleich mit einzubeziehen.

Verfahren in Staatsschutz- und Terrorstrafsachen werden im amerikanischen Recht damit im Wesentlichen vor zwei Gerichten geführt. Bei Straftaten im Inland sind die zivilen Strafgerichte zuständig, welche maßgeblich an die Handlungen der Betroffenen anknüpfen.[83] Die Militärkommissionen orientieren ihre Zuständigkeit am Status des Betroffenen und widmen sich der Verurteilung von im Ausland durch Ausländer begangenen Terrorstraftaten.

II. Produzenten von „Geheimdienstinformationen“

Der amerikanische Geheimdienstsektor ist einer der größten weltweit.[84] Nach offiziellen Angaben umfasst er 17 Behörden.[85] Zudem verfügt eine Vielzahl amerikanischer Behörden über nachrichtendienstliche Abteilungen, sodass der Kreis der tatsächlich mit geheimdienstlichen Tätigkeiten betrauten Einrichtungen auf ca. 60 Behörden geschätzt wird.[86]

---

[81] Zur Definition des *enemy combatant* vgl. Memorandum for the Secretaries of the Military Departments Chairman of the Joint Chiefs or Staffs Under Secretary of Defense for Policy vom 14. Juli 2006, S. 3: “an individual who was part of or supporting Taliban or al Qaida forces, or associated forces that are engaged in hostilities with the United States or its coalition partners”. Vgl. weiterhin 10 U.S.C. § 948a (7)(A).

[82] Dies ergibt sich bereits aus 10 U.S.C. § 948c. Anders ist dies bei der sog. *preventive detention*, vgl. *Kris,* J. Nat’l Sec. L. & Pol’y (5) 2011, S. 57f.

[83] Ebenfalls zur teilweisen verbleibenden Zuständigkeit des nationalen Strafverfahrensrechts vgl. *Chesney,* in: Commission of Inquiry, S. 83 Fn. 2.

[84] Vgl. *Daun*, Auge um Auge, S. 143.

[85] Vgl. zur offiziellen Zahl http://intelligence.gov/about-the-intelligence-community/ [Stand: 1.5.2012].

[86] So etwa das Energie-, Außen- und Finanzministerium; vgl. bei *Droste,* Nachrichtendienste, S. 85; *Jäger/Daun,* in: Borchert, S. 60. Vertiefend zu den einzelnen Einheiten vgl. *Kris/Wilson,* § 1:6, S. 19ff.

A. Die klassischen amerikanischen Dienste

Die klassischen Produzenten von Geheimdienstinformationen und deren Aufgaben werden in der präsidialen Verfügung E.O. 12333 von 2008 aufgelistet.[87] Den dort genannten Behörden obliegt die Beobachtung von Ereignissen, die zum Schutz der nationalen Sicherheit und der auswärtigen Beziehungen notwendig sind.[88] Ihr Zusammenschluss wird als *Intelligence Community* (IC) bezeichnet. Ergänzend wurden mit den Regeln des *Director of National Intelligence* (DNI), des *Attorney General* und den 50 U.S.C. §§ 401–442b *(National Security)* und 50 U.S.C. §§ 1801–1885c *(Foreign Intelligence Surveillance)* gemeinsame Vorschriften aufgestellt, die sich mit der geheimdienstlichen Informationserhebung befassen.[89] Im Übrigen sind die Kompetenzvorschriften stark verstreut. Die einzelnen Dienste können überwiegend den Bereichen der Inlandsaufklärung, der Auslandsaufklärung und der militärischen Aufklärung zugeordnet werden.[90]

1. Die Inlandsaufklärung, insbesondere FBI und DHS

Die amerikanische Sicherheitsarchitektur kennt keinen Inlandsgeheimdienst im Sinne einer verselbstständigten Einrichtung. Jedoch ist eine Vielzahl an Behörden mit der Inlandsaufklärung betraut.[91] Stellvertretend werden die *Intelligence Units* des *Federal Bureau of Investigation* (FBI) und des *Department of Homeland Security* (DHS) vorgestellt.

a) FBI-Einheiten

Das FBI geht auf das im Jahre 1908 gegründete *Bureau of Investigation* zurück und war ursprünglich als bundespolizeiliche Ermittlungsbehörde konzipiert.[92] Es

---

[87] Vgl. E.O. 12333 in der Fassung von 2008 unter Punkt 1.7. Die ursprüngliche E.O. 12333 (4.12.1981) wurde durch die E.O. 13284 (2003), 13355 (2004) und 13470 (2008) berichtigt. Eine weitere Auflistung findet sich in 50 U.S.C. § 401a (4). Eine Executive Order ist eine bindende Verfügung des Präsidenten mit Gesetzeskraft.

[88] Vgl. http://www.dni.gov/definition_IC.htm [Stand: 1.5.2012].

[89] Teile der genannten Richtlinien unterliegen allerdings der Geheimhaltung. So etwa die mittlerweile abgelösten Richtlinien des *Attorney General*s in Bezug auf FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines) von 2003. Zu finden unter http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf [Stand: 1.5.2012]. Deren vollständige Freigabe sollte erst am 31.10.2028 erfolgen.

[90] Vgl. *Masse,* CRS 2006, S. 5. Daneben existiert der Bereich der *homeland security intelligence*. Dieser weist Überschneidungen zu allen drei *intelligence*-Dimensionen auf und wird vorliegend der Inlandsaufklärung zugewiesen.

[91] Zu den verschiedenen Akteuren der Inlandsaufklärung vgl. *Posner,* S. 55; *Rascoff,* S. Cal. L. Rev. (83) 2010, S. 593.

[92] Vgl. hierzu den offiziellen Internetauftritt des FBI unter http://www.fbi.gov/about-us/history/brief-history/brief-history [Stand: 1.5.2012] sowie *Kris/Wilson,* § 1:7, S. 28ff.

wurde im Juli 1932 in *United States Bureau of Investigation* und 1935 schließlich in *Federal Bureau of Investigation* unbenannt.[93] Die maßgeblichen Rechtsgrundlagen für die polizeiliche Arbeit finden sich im 18. und 28. *Title* des U.S.C.[94] Generell obliegt dem FBI die Kriminalitätsaufklärung von Bundesstraftaten und grenzüberschreitenden Straftaten innerhalb der USA, sofern diese nicht ausdrücklich anderen Behörden zugewiesen sind.[95] Von diesem Auftrag werden sowohl die Aufklärung begangener als auch die Verhinderung künftiger Straftaten erfasst.[96] Organisatorisch untersteht das FBI dem Justizministerium.[97]

Das FBI ist allerdings nicht auf diese bundespolizeiliche Tätigkeit beschränkt. Seit dem 12. September 2005 existiert mit dem *National Security Branch* sogar ein unabhängiger Geheimdienstzweig, der mit seinen Abteilungen zur Terrorismusbekämpfung und Gegenspionage klassische geheimdienstliche Aufgabenfelder abdeckt.[98] Das FBI ist insofern insgesamt mit der Erhebung von *foreign intelligence* und *counterintelligence* betraut.[99] Die geheimdienstlichen Beobachtungsfelder erfassen unter anderem die Aufklärung von Bedrohungen der nationalen Sicherheit durch den internationalen Terrorismus, Spionagetätigkeiten oder sonst feindliche Bestrebungen, die von ausländischen Staaten oder Organisationen drohen.[100] Gegenstand der Informationserhebung sind Fähigkeiten, Absichten und Aktivitäten ausländischer Regierungen, Organisationen, Personen oder Terroristen, sofern dieses Wissen von außen- und sicherheitspolitischer Bedeutung ist.[101] Die durch das FBI erhobenen Erkenntnisse werden dem Präsidenten sowie sonstigen exekutiven

---

[93] Vgl. hierzu den offiziellen Internetauftritt des FBI unter http://www.fbi.gov/about-us/history/brief-history/brief-history [Stand: 1.5.2012]. Durch die Umbenennung sollten Verwechslungen mit dem *Bureau of Prohibition*, einer Abteilung des Justizministeriums, verhindert werden.

[94] Vgl. *Grunwald,* S. 35. So u.a. in 28. U.S.C. § 531 bis § 540C (Verfolgung von Bundesstraftaten), 18. U.S.C. § 3052 (Tragen von Feuerwaffen, Durchsuchungsbefugnisse).

[95] Vgl. nach 28 U.S.C. § 533. Ebenso *Droste,* Nachrichtendienste, S. 84, die das FBI mit dem BKA vergleicht, da es „nur für die Verfolgung solcher Bundesstraftaten zuständig [ist], die nicht anderweitig zugewiesen sind".

[96] Vgl. *Grunwald,* S. 36.

[97] 28 U.S.C. § 531.

[98] Vgl. hierzu den offiziellen Internetauftritt unter http://www.dni.gov [Stand: 1.5.2012] sowie *Kris/Wilson,* § 1:7; *Rascoff,* S. Cal. L. Rev. (83) 2010, S. 593.

[99] Vgl. zur Definition die Mukasey Guidelines 2008, S. 8, sowie 50 U.S.C. § 401a. Danach umfasst der Begriff *foreign intelligence* "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities". Der Begriff *counterintelligence* erfasst dagegen "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities". Ebenso *Grunwald,* S. 38.

[100] Vgl. E.O. 12333 in der Fassung von 2008 unter Punkt 1.7 (g). Mukasey Guidelines 2008, S. 7; vgl. ebenso *Arzt,* in: Graulich/Simon, S. 256.

[101] Mukasey Guidelines 2008, S. 9.

Entscheidungsträgern zur Verfügung gestellt, um Beeinträchtigungen der nationalen Sicherheit sowie Aktivitäten des Terrorismus verhindern zu können.[102] Zu diesem Zweck ist dem FBI der frühzeitige Einsatz eingriffsintensiver und nachrichtendienstlicher Methoden (HUMINT, SIGINT) gestattet.[103] Das FBI erweist sich insofern als die führende inländische Ermittlungsbehörde bei Bedrohungen der nationalen Sicherheit und der Terrorismusbekämpfung.[104]

Die zentralen geheimdienstlichen Befugnisse ergeben sich aus der bereits genannten E.O. 12333 von 2008 unter Punkt 1.7 (g), den 50 U.S.C. §§ 401–442b *(national security)*, dem *Foreign Intelligence Surveillance Act* (FISA) in 50 U.S.C. §§ 1801–1885c sowie den Richtlinien des *Attorney General Mukasey* zum Bereich der *Domestic FBI Operations* von 2008 *(Mukasey Guidelines 2008)*.[105] Eine ausdrückliche Ermächtigung für rein inländische Geheimdienstaktivitäten des FBI, also den Bereich der *domestic intelligence investigations,* fehlt.[106] Allerdings ergibt sich bereits aus den Mukasey Guidelines 2008, dass die geheimdienstlichen Aufgaben des FBI nicht lediglich Tätigkeiten mit Auslandsbezug, sondern auch rein innerstaatliche Sachverhalte erfassen können.[107] Lediglich für elektronische Überwachungsmaßnahmen ohne Auslandsbezug ist ein Rückgriff auf die Vorgaben der polizeilichen Ermächtigungen erforderlich.[108] In funktionaler Hinsicht kann das FBI damit als Produzent von Geheimdienstinformationen eingestuft werden.

b) DHS-Behörden

Die Inlandsaufklärung wird zudem durch die Geheimdiensteinheiten des *Department of Homeland Security* (DHS) wahrgenommen. Dieses Heimatschutzministerium wurde als Reaktion auf die Terroranschläge in New York als Koordi-

---

[102] Mukasey Guidelines 2008, S. 8.

[103] Vgl. insbesondere den Bereich des *threat assessment*; vgl. zudem den offiziellen Internetauftritt unter http://www.fbi.gov/ about-us/intelligence/disciplines [Stand: 1.5.2012].

[104] Vgl. Mukasey Guidelines 2008, S. 5; *Chesney,* in: Commission of Inquiry, S. 86; *Johnson,* I/S: J.L. & Pol’y for Info. Soc’y (5:3) 2010, S. 438; *McNamara,* in: Markle Foundation, S. 89.

[105] Vgl. *Michael B. Mukasey*, U.S. Dep’t Of Justice, The Attorney General’s Guidelines For Domestic FBI Operations*,* abrufbar unter http://www.justice.gov/ag/readingroom/guidelines.pdf [Stand: 1.5.2012]. Vertiefend *Berman*, S. 21; *Johnson*, I/S: J.L. & Pol’y for Info. Soc’y (5:3) 2010, S. 438ff; *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 151ff. Diese gelten für sämtliche inländischen Tätigkeiten, d.h. sowohl für den Geheimdienst- als auch den Strafverfolgungssektor. Sie lösen die *NSI Guidelines* von 2003 ab.

[106] Vgl. *Grunwald,* S. 38ff.

[107] Siehe Mukasey Guidelines 2008, S. 9; vgl. *Grunwald,* S. 40, 72. Diese allerdings mit Verweis auf den Begriff der umstürzlerischen Aktivitäten, die sog. *subversive activities*. Dieser Begriff findet sich in den aktuell geltenden Richtlinien nicht mehr.

[108] So der Verweis in den Mukasey Guidelines 2008 unter Punkt V.A., S. 32. In 18 U.S.C. § 2511(2)(f) wird der abschließende Charakter der Ermächtigungen für inländische Kommunikationsüberwachung *(wire, oral, electronic)* abseits des FISA betont.

nierungsstelle für die Terrorabwehr innerhalb der USA auf der Grundlage des *Homeland Security Act 2002* geschaffen. Aufgabe dieser Behörde ist der Schutz der amerikanischen Bevölkerung und des amerikanischen Staatsgebietes vor terroristischen Bedrohungen. Dieses Ziel soll durch die Zusammenführung und Koordinierung zahlreicher Bundesbehörden unter einem Dach erreicht werden.[109] Organisatorisch verfügt das DHS mit dem *Office of Intelligence and Analysis* (I&A) und dem Nachrichtendienst der Küstenwache *(Coast Guard Intelligence)* über zwei eigenständige Geheimdiensteinheiten.[110] Dem I&A obliegt als zentrales Analysezentrum die Sammlung und Auswertungen von Informationen, die von anderen Einrichtungen des DHS erlangt wurden und zur Identifikation und Bewertung künftiger Bedrohungen für die USA notwendig sind.[111] Es fungiert zudem als eine Schaltstelle für den Informationsaustausch zwischen den anderen Mitgliedern des IC, des DHS und sonstiger Regierungseinrichtungen.[112] Mit seiner Arbeit unterstützt es die Entscheidungsträger unter anderem in Bezug auf die Grenzsicherung und Einwanderungspolitik, das Erkennen von Extremisten im Inland sowie die Terrorismusbekämpfung.[113] Es werden damit zwar Teile der Geheimdienstdefinition erfüllt, dennoch zeichnen sich das DHS beziehungsweise das I&A mehr durch Koordinierungs- und Analysefunktionen als durch eigene Ermittlungsbefugnisse aus. Eine Erzielung eigenständiger Erkenntnisse durch die Einbeziehung des DHS beziehungsweise des I&A in die Untersuchung ist nicht zu erwarten, sodass diese nachfolgend außer Betracht bleiben können.

2. Die Auslandsaufklärung, insbesondere CIA

Die *Central Intelligence Agency* (CIA) wurde als Nachfolgeorganisation des primär militärisch orientierten *Office of Strategic Services* mit dem *National Security Act* von 1947 begründet.[114] Aktuell ist die CIA für die zivile Auslandsaufklärung zuständig. Die maßgeblichen Rechtsgrundlagen finden sich in der E.O. 12333 von 2008 unter Punkt 1.7 (a), dem National Security Act von 1947, den 50 U.S.C. §§ 403-4, 403-4a, 403a bis 403s sowie den Ermächtigungen durch den

---

[109] Vgl. hierzu *Zöller,* Terrorismusstrafrecht*,* S. 202.

[110] Vgl. hierzu http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm [Stand: 1.5.2012], sowie *Rascoff,* S. Cal. L. Rev. (83) 2010, S. 580, 593. Die Geheimdiensteinheit der Küstenwache ist eher dem militärischen Bereich zuzuordnen, vgl. http://www.uscg.mil/top/missions/[Stand: 1.5.2012] sowie 14 U.S.C.

[111] Seine Informationen bezieht es vor allem aus öffentlich zugänglichen Quellen, vgl. E.O. 12333 von 2008 Punkt 1.7 (i)(1).

[112] So der offizielle Internetauftritt des DHS unter http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm [Stand: 1.5.2012].

[113] Vgl. ODNI Guide 2009, S. 48f.

[114] Vgl. *Hörauf,* S. 290.

Präsidenten.[115] Organisatorisch untersteht die CIA direkt dem Präsidenten. Im Gegensatz zu den anderen Diensten ist kein Fachministerium zwischengeschaltet.[116] Die wesentlichen Aufgaben der CIA werden in 50 U.S.C. § 403-4a(d)(1) bis (3) präzisiert. Der CIA obliegt danach die Sammlung von *foreign intelligence* und *counterintelligence* unter Einsatz menschlicher Quellen und damit im Schwerpunkt die heimliche Informationserhebung in nationalen Sicherheitsfragen.[117] Die gewonnenen Erkenntnisse werden auf ihre Relevanz für die nationale Sicherheit geprüft und dem Präsidenten, dem Vizepräsidenten, dem NSC und den Mitgliedern des Kabinetts zur Verfügung gestellt.[118] Schließlich koordiniert die CIA die Durchführung von Beobachtungsmaßnahmen mittels HUMINT im Ausland und stellt deren effektive Durchführung sicher. Ein wichtiges organisatorisches Element bildet die CIA-Abteilung *National Clandestine Service* (NCS). Diese ist für die Sammlung, Koordination und Bewertung von geheimen HUMINT-Operationen sowie die Weiterleitung der daraus resultierenden Erkenntnisse zuständig.[119] Darüber hinaus kann die CIA mit den sogenannten *covert actions* aktive Auslandsoperationen sowie elektronische Auslandsaufklärung durchführen.[120] Nicht gestattet sind demgegenüber der Einsatz von Polizei-, Zwangs- und Strafverfolgungsmaßnahmen, die Wahrnehmung inländischer Sicherheitsfunktionen sowie die elektronische Überwachung im Inland.[121] Insgesamt erfüllt die CIA sämtliche Anforderungen der Geheimdienstdefinition.

3. Die militärische Aufklärung, insbesondere DIA und NSA

Die militärische Aufklärung nimmt den größten Bereich des amerikanischen Geheimdienstsektors ein. Zentrale Akteure sind die *Defense Intelligence Agency* (DIA) und die *National Security Agency* (NSA), welche beide dem Verteidigungsministerium zuzuordnen sind.[122] Die DIA wurde im Jahr 1961 gegründet und bildet

---

[115] Die Ermächtigungen in 50 U.S.C. gehen vor allem auf den CIA Act von 1949 zurück und befreien die CIA von vielen Beschränkungen, vgl. *Hörauf,* S. 290.

[116] Vgl. *Hörauf,* S. 289.

[117] Vgl. *Daun*, Auge um Auge, S. 144; *Kris/Wilson,* § 1:6, S. 20f.

[118] Die CIA nimmt damit im analytischen Bereich eine Vormachtstellung ein, vgl. *Kris/Wilson,* § 1:6, S. 20.

[119] So u.a. der offizielle Internetauftritt der CIA unter https://www.cia.gov/offices-of-cia/clandestine-service/index.html [Stand: 1.5.2012]; ebenso *Hörauf,* S. 318.

[120] Vgl. E.O. 12333 von 2008 unter Punkt 1.7 (a) (4), 2.4 (a); vgl. *Hörauf,* S. 290; *Isenberg,* Cato Policy Analysis 118 (April 7) 1989, S. 1ff.

[121] Vgl. hierzu 50 U.S.C. § 403-4a(d)(1), der vom Verbot von “police, subpoena, or law enforcement powers or internal security functions” spricht. Ebenso E.O. 12333 von 2008 unter Punkt 2.4.(a) sowie *Kris/Wilson,* § 2:11, S. 67ff.

[122] Zudem existieren die *National Geospatial-Intelligence Agency* (NGA) und das *National Reconnaissance Office* (NRO). Die NGA ist für die geografische Aufklärung zuständig, das NRO für die Satellitenaufklärung; vgl. *Daun*, Auge um Auge, S. 145; *Kris/*

als zentrale Koordinierungs- und Auswertungsstelle die Dachorganisation der militärischen Auslandsaufklärung.[123] Primäre Aufgabe der DIA ist die Überwachung und Analyse von *foreign intelligence* und *counterintelligence*.[124] Die DIA bewertet Erkenntnisse, welche ihr durch die verschiedenen Einzeldienste zur Verfügung gestellt werden. Diese Informationen stammen unter anderem von den *Intelligence*-Einheiten der Landstreitkräfte, der Marine und der Luftwaffe. Zudem ist die DIA zur aktiven Gegenspionage befugt.[125]

Ihre Erkenntnisse werden militärischen Entscheidungsträgern, wie dem Verteidigungsminister *(Secretary of Defense)* und dem Vorsitzenden des Vereinigten Generalstabs der Streitkräfte *(Chairman of the Joint Chiefs of Staff)* zur Verfügung gestellt.[126] Die daneben bestehende NSA wurde offiziell im Jahr 1952 gegründet.[127] Sie ist für die Datensicherheit und Kryptologie im Bereich der Kommunikations- und Informationstechnik sowie für die signalerfassende Aufklärung (SIGINT) und Kommunikationsüberwachung (COMINT) zuständig.[128] Im Bereich der Kommunikationsüberwachung beobachtet und analysiert die NSA den Kommunikationsverkehr fremder Regierungen und erhebt damit *foreign intelligence* und *counterintelligence*.[129] Sie ist neben dem FBI die einzige Behörde, der zur Kommunikationsüberwachung der Rückgriff auf den FISA gestattet ist.[130] Mit ihren Informationen und Analysen unterstützt die NSA das Militär, politische Entscheidungsträger und andere Geheimdienste. Sie kann folglich gleichzeitig der militärischen und auslandsspezifischen Aufklärung zugeordnet werden. DIA und NSA erfüllen damit wesentliche Merkmale der Geheimdienstdefinition.

B. Sonstige Produzenten von Geheimdienstinformationen

Neben den klassischen Geheimdiensten finden sich im amerikanischen Sicherheitsrecht weitere Akteure, die bei einer funktionalen Betrachtungsweise dem Produzentenkreis von Geheimdienstinformationen zugeordnet werden können. In die-

---

Wilson, § 1:6, S. 23f. Daneben existieren weitere Einzeldienste, die der DIA zugeordnet sind.

123 Vgl. ODNI Guide 2009, S. 5.

124 Vgl. E.O. 12333 von 2008 unter Punkt 1.7 (b) (1).

125 Vgl. E.O. 12333 von 2008 unter Punkt 1.7 (b) (3).

126 Vgl. E.O. 12333 von 2008 unter Punkt 1.7 (b) (2); ebenso ODNI Guide 2009, S. 5.

127 So der offizielle Internetauftritt der NSA unter http://www.nsa.gov/about/faqs/about_nsa.shtml [Stand: 1.5.2012].

128 Vgl. E.O. 12333 von 2008 unter Punkt 1.7 (c) (8) sowie den offiziellen Internetauftritt des DNI unter http://www.dni.gov/members_IC_3.htm [Stand: 1.5.2012]; vgl. *Daun*, Auge um Auge, S. 145; Ebenso *Kris/Wilson,* § 1:6, S. 20.

129 Vgl. E.O. 12333 von 2008 unter Punkt 1.7 (c) (1).

130 Vgl. *Hörauf,* S. 292; *Kris/Wilson,* § 1:6, S. 23f.

sem Zusammenhang sind überraschenderweise die Polizei- und Strafverfolgungsbehörden der Einzelstaaten und Gemeinden zu nennen.[131] Deren zumindest teilweise Zuordnung zum Geheimdienstsektor ist spätestens seit den Änderungen durch den *USA PATRIOT Act* von 2001 gerechtfertigt. Durch diesen wurden die Strafverfolgungsbehörden offiziell in die Bekämpfung des internationalen Terrorismus und die Herstellung der nationalen Sicherheit integriert.[132] Die Betrauung mit proaktiven Aufgaben war aufgrund der im amerikanischen Sicherheitsrecht fehlenden Trennung zwischen repressiven und präventiven Aufgaben möglich.[133] Vor allem die Größe und die guten Kontaktmöglichkeiten dieser Behörden zu den Gemeinden und lokalen Polizeibehörden waren bei dieser Entscheidung ausschlaggebend. Die einzelstaatlichen Strafverfolgungsbehörden verfügen über 1,1 Million Mitarbeiter, wovon etwa 200.000 mit Fragen der Terrorbekämpfung beschäftigt sind.[134] Viele dieser Behörden verfügen sogar über große *counterterrorism intelligence*-Abteilungen. Dem stehen vergleichsweise nur ca. 36.000 Mitarbeiter beim FBI gegenüber, wovon ca. 14.000 als *Special Agents* tätig sind.[135] Die Einbeziehung der lokalen Behörden in die *intelligence*-Beschaffung eröffnet damit enorme Ermittlungskapazitäten. Sie sind zudem zur Teilnahme an geheimdienstlichen Ermittlungen und zur Kooperation mit der *Intelligence Community* befugt, sodass das von ihnen erzielte Wissen weitgehend auch anderen Geheimdienst- und Strafverfolgungsbehörden zur Verfügung steht.[136] Diese *state* beziehungsweise *local law enforcement agencies* sind damit zwar keine offiziellen Mitglieder der *Intelligence Community*, dennoch tragen sie mit ihren Ermittlungen wesentlich zur Produktion von Geheimdienstinformationen bei.[137] Von Sicherheitsexperten wird dieser Sektor dementsprechend als einer der wichtigsten Produzenten von Geheimdienstinformationen angesehen.[138] Hierbei ist allerdings zu berücksichtigen, dass sowohl das Verständnis von *intelligence* als auch die Standards von Einzelstaat zu Einzelstaat erheblich variieren.

---

131 Vgl. *Hulnick,* IJIC (22) 2009, S. 581; *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 80; *Treverton,* Reorganizing, S. 23. A.A. *Carter,* S. 17, in Bezug auf *national security intelligence.*

132 Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 5, 8, 80, allerdings allgemein zur LEC.

133 Vgl. *Carter*, S. 9; *Markwordt Skehan,* S. 100. Vertiefend und kritisch *Ross,* Surveillance, S. 4. Bereits davor wurde die umfassende Bestrafung von (Vorbereitungs-) Delikten zur Verhinderung von schwerwiegenden Sekundärdelikten genutzt, etwa durch das *conspiracy law* oder den sog. *material support for terrorist organizations* nach 18 U.S.C. 2339A(a); vgl. *Chesney,* in: Commission of Inquiry, S. 87ff.

134 Vgl. http://bjs.ojp.usdoj.gov/content/pub/pdf/csllea08.pdf [Stand: 1.5.2012].

135 Vgl. http://www.fbi.gov/about-us/quick-facts [Stand: 1.5.2012]. *Masse,* CRS 2003, S. 16, geht im Jahr 2003 noch von 12.000 Agenten aus.

136 Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 9; vgl. zu den Kooperationsformen Teil 3, III.A.2.

137 Vgl. *Treverton,* Reorganizing, S. 23.

138 Vgl. hierzu *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 80.

C. Zwischenergebnis zu Produzenten

Im amerikanischen Sicherheitssektor ist eine Vielzahl von Behörden mit geheimdienstlichen Aufgaben betraut. Die offiziellen Produzenten von Geheimdienstinformationen sind primär auf Bundesebene angesiedelt. Diese werden in ihrer Arbeit teilweise durch Ermittlungen der Strafverfolgungsbehörden unterstützt. Trotz seiner Zwitterstellung hat sich das FBI im Bereich der Inlandsaufklärung als *chief domestic intelligence agency* der USA herauskristallisiert.[139] Für die Bedürfnisse des vorliegenden Rechtsvergleichs werden daher die geheimdienstlichen Ermittlungsmöglichkeiten des FBI als Grundmodell herangezogen.

III. Auswirkungen der amerikanischen Sicherheitsarchitektur

Die nächsten Abschnitte widmen sich der Einordnung geheimdienstlicher Ermittlungen in die amerikanische Sicherheitsarchitektur (A.) und deren Auswirkungen auf die strafprozessuale Nutzung von Geheimdienstinformationen (B.).

A. Entwicklung der Sicherheitsarchitektur

1. Ausgangslage nach 1945

Der *National Security Act* von 1947 bildet den Grundstein für das amerikanische Geheimdienstwesen und prägt die Einordnung der Dienste bis heute. Zum damaligen Zeitpunkt waren geheimdienstliche Tätigkeiten vor allem auf das Ausland ausgerichtet. Hintergrund war ein Verständnis, wonach Gefährdungen der nationalen Sicherheit vor allem durch ausländische Mächte drohten.[140] Die Aufklärung dieser Bedrohung wurde primär der CIA übertragen, der umgekehrt der Einsatz polizeilicher Zwangs- und Strafverfolgungsbefugnisse sowie die Wahrnehmung von Sicherheitsfunktionen im Inland verboten war.[141] Diese territoriale und kompetenzrechtliche Beschränkung wurde offiziell auf die zum damaligen Zeitpunkt bestehende Furcht vor „gestapoähnlichen Strukturen“ zurückgeführt. Das Missbrauchspotential verschmolzener geheimdienstlicher und polizeilicher Strukturen

---

[139] Vgl. *Chesney*, in: Commission of Inquiry, S. 86; *Johnson,* I/S: J.L. & Pol’y for Info. Soc’y (5:3) 2010, S. 438.

[140] Die zentrale Bedrohung schien damals durch die Sowjetunion zu bestehen; vgl. insgesamt *Swire,* Vill. L. Rev. (51) 2006, S. 955; *Zöller,* Terrorismusstrafrecht, S. 200.

[141] Siehe 50 U.S.C. § 403-4a(d)(1); vgl. *Manget,* Stan. L. & Pol’y Rev. (17) 2006, S. 416.

war am Beispiel der deutschen Gestapo und des russischen KGB bereits deutlich geworden und sollte für amerikanische Behörden verhindert werden.[142] Inoffiziell ist diese Begrenzung jedoch zu einem erheblichen Anteil dem damaligen Einfluss des FBI geschuldet. Dieses hatte sich bei der Gründung der CIA im Jahr 1947 als eigenständige Behörde bereits etabliert und wollte seine in Inlandsfragen bestehende Vormachtstellung verteidigen.[143] Bei genauerer Betrachtung nahm das FBI jedoch seinerseits nicht nur rein polizeiliche Aufgaben wahr. Spätestens seit 1936 war es zusätzlich mit der Beobachtung umstürzlerischer Bestrebungen betraut.[144] Diese Erweiterung auf zumindest teilweise geheimdienstliche Aufgabenfelder sollte eine bessere Kontrolle der aus Europa überschwappenden kommunistischen und nationalsozialistischen politischen Bewegungen ermöglichen.[145] Diese ursprünglich auf die politisch angespannte Zeit vor dem Krieg zugeschnittene Erweiterung wurde auch in den Folgejahren beibehalten.[146] Mit dem FBI entstand damit eine hybride Institution, die faktisch sowohl geheimdienstliche als auch polizeiliche Aufgaben im Inland wahrnehmen durfte. Rein definitorisch wurden die Überschneidungen zum geheimdienstlichen Aufgabenbereich dadurch umgangen, dass das FBI sämtliche verdächtige Aktivitäten im Inland als Straftat einstufte.[147] Inländische Bedrohungen wurden somit primär als strafrechtliche Fälle verstanden, zu deren Aufklärung das FBI befugt war.[148] Die ursprüngliche Einordnung geheimdienstlicher Ermittlung in die amerikanische Sicherheitsarchitektur war damit maßgeblich durch die Unterscheidung zwischen inländischen und ausländischen Aktivitäten bestimmt.[149]

2. Entwicklung der Sicherheitsarchitektur bis heute

Die im Ausgangspunkt bestehende Trennung wurde in den Folgejahren schrittweise aufgeweicht. Der bisherige Auslandsfokus der Geheimdienste konnte mit der Zunahme inländischer und grenzüberschreitender Bedrohungslagen nicht aufrechterhalten werden.[150] Insbesondere durch den aufkommenden internationalen Drogenhandel und Flugzeugterrorismus wurde deutlich, dass Gefahren für die USA

---

142 Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 335; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 416; *Treverton,* Intelligence, S. 1.

143 Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 335; *Hulnick,* IJIC (22) 2009, S. 572.

144 Vgl. *Masse,* CRS 2003, S. 5.

145 Vgl. *Masse,* CRS 2003, S. 4f.

146 Vgl. *Masse,* CRS 2003, S. 5f.

147 Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 335.

148 So *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 335; *Rozen,* in: Markle Foundation, S. 114f.

149 Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 335f.

150 Vgl. *Swire,* Vill. L. Rev. (51) 2006, S. 955, 957.

nicht mehr nur von ausländischen Staaten mit staatlichen Mitteln drohten. Die neuen Bedrohungslagen gingen vielmehr von einer Vielzahl kleiner, oft kaum sichtbarer Gruppierungen mit neuen Angriffsmitteln aus. Diese Entwicklung führte zu einem Umdenken im Bereich der Inlandsaufklärung.[151] In der Folge wurde erstmals offiziell die Notwendigkeit einer geheimdienstlichen Aufklärung im Inland anerkannt, allerdings ohne dass die Struktur oder die Kontrolle inländischer Geheimdienstaktivitäten eindeutig gesetzlich fixiert wurde.

Mangels konkreter gesetzlicher Leitlinien kam es daher zwischen 1947 und 1975 im Bereich der Inlandsaufklärung zu zahlreichen Missbrauchsfällen und kompetenzwidrigen Übergriffen durch die Geheimdienste.[152] Diese und die ungeklärte Rechtslage waren Gegenstand gerichtlicher und parlamentarischer Auseinandersetzungen. In der sogenannten *Keith*-Entscheidung im Jahr 1972 wurden erstmals die unterschiedlichen Bedürfnisse von strafrechtlichen und geheimdienstlichen Ermittlungen zum Schutz der nationalen Sicherheit anerkannt.[153] In seinem Urteil betonte das Gericht die grundsätzliche Bindung von *domestic intelligence investigations* (DII) an die Vorgaben des vierten Verfassungszusatzes und damit das Erfordernis einer richterlichen Kontrolle.[154] Allerdings erkannte es gleichzeitig die besonderen Bedürfnisse geheimdienstlicher Ermittlungen an und berechtigte den Gesetzgeber zum Erlass einer Sonderermächtigung. In dem Urteil heißt es unter anderem ausdrücklich:

> we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of ordinary crime.[155]

Nach diesen Ausführungen ist der Gesetzgeber durchaus berechtigt unterschiedliche Standards für geheimdienstliche und strafrechtliche Ermittlungen, das heißt *intelligence* und *law enforcement activities,* aufzustellen, solange die Rechte der Bürger ausreichend gewahrt bleiben. Hinsichtlich Ermittlungen mit Auslandsbezug, den sogenannten *foreign intelligence investigations* (FII), ließ das Gericht eine Entscheidung indes offen. Daneben waren die Missbrauchsfälle im Jahr 1975 Gegenstand von Untersuchungsausschüssen des US-Senats, dem sogenannten *Church Committee*, und des Repräsentantenhauses, dem sogenannten *Pike Commit-*

---

151 Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 335.

152 Vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 149.

153 Siehe *United States v. U.S. District Court*, 407 U.S. 297 (S. Ct. 1972); vgl. *Arzt,* in: Graulich/Simon, S. 254f; *Birkenstock,* Geo. L. J. (80) 1992, S. 863; *Kris/Wilson,* § 3:6.

154 Vgl. *Arzt,* in: Graulich/Simon, S. 254f; *Hall,* Wake Forest L. Rev. (41) 2006, S. 88; *Vervaele,* Utrecht L. Rev. (1) 2005, S. 5.

155 Siehe *United States v. U.S. District Court*, 407 U.S. 297, 322 (S. Ct. 1972); vgl. zudem *Fenske,* NULR (102) 2008, S. 354f.

tee.[156] Diese deckten zahlreiche Rechtsbrüche und Defizite auf, darunter unter anderem den Einsatz unzulässiger Ermittlungsmethoden, die Überwachung untauglicher Ziele, die missbräuchliche Verfolgung politischer Ziele sowie das Fehlen ausreichender gesetzlicher Grundlagen.[157] Gerade die umfassende Überwachung unter Umgehung des Richtervorbehalts wurde als Bedrohung politischer Freiheiten und Verletzung des ersten Verfassungszusatzes wahrgenommen.[158]

Als Reaktion auf die offengelegten Missstände erließ der Kongress 1978 den *Foreign Intelligence Surveillance Act* (FISA), der Ermittlungen zum Schutz vor ausländischen und internationalen Bedrohungen und damit die sogenannten *foreign intelligence investigations* (FII) gestattete.[159] Inhaltlich sollte der FISA die bislang weitläufige auslandsbezogene Inlandsaufklärung (FII) in dreierlei Hinsicht einschränken. Erstens sollten verbindliche Erhebungsstandards festgelegt, zweitens etwaige Zielobjekte auf ausländische Mächte begrenzt und drittens die parlamentarische und gerichtliche Kontrolle durch Berichtspflichten und die Errichtung des FISC *(Federal Intelligence and Surveillance Court)* als Sondergericht ausgebaut werden.[160] Der Kongress begnügte sich bei seinen Reformbestrebungen allerdings mit dem Bereich der FII. Ein dem FISA korrespondierendes Gesetzeswerk für den Bereich der DII und damit geheimdienstliche Beobachtungen rein inländischer Sachverhalte wurde nicht geschaffen.[161] In der Folge wurde die davor maßgebliche Unterscheidung zwischen strafrechtlichen und geheimdienstlichen Ermittlungen *(LEC vs. IC)* durch den Gegensatz strafrechtlicher Ermittlungen zur auslandsbezogenen Inlandsaufklärung ersetzt *(LEC vs. FII)*.[162]

Die sich anschließende Entwicklung wurde maßgeblich durch die Vorgaben des FISA und seiner wechselhaften gerichtlichen Auslegung geprägt. In den 1980er und frühen 1990er Jahren entwickelten die Gerichte den sogenannten *primary purpose*-Test, der die Auslegung des FISA und die Einordnung geheimdienstlicher Ermittlungen über Jahre hinweg bestimmte.[163] Nach diesem Test durften auf der

---

[156] Vgl. http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm [Stand: 1.5.2012].

[157] Vgl. hierzu im Einzelnen *Kris/Wilson,* § 2:2 bis § 2:6.

[158] Vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 149.

[159] Vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 149; *Grunwald,* S. 76; *Zabel/Benjamin,* S. 77, sowie unter Teil 1, II.A.2.

[160] Vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 149f.

[161] Diese fehlt bis heute, sodass für DII die verfassungsrechtlichen Grenzen gelten.

[162] IC steht dabei für Intelligence Community, LEC für Law Enforcement Community und FII für Foreign Intelligence Investigations.

[163] Vgl. *Kris/Wilson,* § 3:7, S. 106; *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 224ff; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 417. Oftmals wird die Entscheidung *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980) als Grundlage dieses Tests zitiert, vgl. *In re Sealed Case*, 310 F.3d 717, 725ff, 742f (FISCR 2002); *Glick,* Harv. NSJ (1) 2010, S. 102.

Grundlage des FISA erhobene Erkenntnisse zu Strafverfolgungszwecken nur herangezogen werden, wenn der primäre Zweck der ursprünglichen Informationserhebung in der Auslandsaufklärung lag. Primärer Erhebungszweck mussten folglich *foreign intelligence* (FI) oder *foreign counterintelligence* (FCI) sein. Die Bindung an den primären Zweck der Maßnahme wurde aus dem damaligen Wortlaut des FISA gefolgert, der von „the purpose" sprach.[164] Der gezielte Einsatz des FISA zu Strafverfolgungszwecken war nach dieser Interpretation als Verstoß gegen den Richtervorbehalt des vierten Verfassungszusatzes unzulässig.

Von diesem Verständnis ausgehend wurde eine den Informationsaustausch begrenzende verwaltungsrechtliche Hürde aufgebaut, die in der Folge als *wall* bekannt wurde.[165] Die *wall* trennte in formaler Hinsicht den Geheimdienst- und Strafverfolgungssektor sowie inlands- und auslandsspezifische Aufgabenfelder.[166] Durch diese Trennung wurde der auslandsbezogenen Inlandsaufklärung (FII) eine rechtliche Sonderstellung zuerkannt, wohingegen die geheimdienstliche Aufklärung rein inländischer Sachverhalte (DI) mangels eigenständiger Kodifikation weiterhin den allgemeinen strafrechtlichen Regeln unterlag und bis heute unterliegt.[167] Durch die *wall* war allerdings die FII komplett von übrigen Ermittlungsbereichen getrennt, während sich die DII vollständig in den strafrechtlichen Kontext integrierten. Diese Unterscheidung innerhalb geheimdienstlicher Ermittlungen kommt bis heute in unterschiedlichen Anordnungskompetenzen und abweichenden Ermächtigungsgrundlagen zum Ausdruck.[168] Während strafrechtliche Ermittlungen und DII an den Richtervorbehalt des vierten Verfassungszusatzes gebunden sind, können Maßnahmen der FII durch den geheim tagenden FISC angeordnet werden.[169] Ebenso verhält es sich im Bereich der Telekommunikations- und Wohnraumüberwachung. Diese richtet sich zu Strafverfolgungszwecken und Zwecken der DII nach 18 U.S.C. §§ 2510–2522 (Title III[170]). Demgegenüber unterliegt die inländische Auslandsüberwachung der FII den Regeln des FISA in den 50 U.S.C. §§ 1801–1862. Die hieraus resultierenden unterschiedlichen Schutzstandards für inlands-

---

164 Vgl. *Standler*, S. 17f.

165 Vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 94; *Kris/Wilson,* § 3:7.

166 Vgl. *Roach*, Challenges, S. 41; *Treverton,* Intelligence, S. 2.

167 Vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 150.

168 Dies gilt selbst innerhalb des FBI; vgl. *Becker,* RIDP/IRPL 2009, S. 348; *Johnson,* I/S: J.L. & Pol'y for Info. Soc'y (5:3) 2010, S. 439.

169 Vgl. *Vervaele,* Utrecht L. Rev. (1) 2005, S. 5.

170 Diese Befugnis basiert auf dem Omnibus Crime Controle and Safe Streets Act von 1968 (Abk. Title III), der durch den Electronic Communications Privacy Act von 1984 (ECPA) und den Communications Assistance for Law Enforcement Act von 1994 (CALEA) ergänzt wurde; vgl. *Arzt,* in: Graulich/Simon, S. 249f.

und auslandsspezifische Geheimdienstmaßnahmen wurden in verschiedenen Urteilen bestätigt.[171]

In den Jahren von 1995 bis 2000 wurde diese Trennung weiter gefestigt.[172] In den Memoranden der Justizminister vom 19. Juli 1995 *(Memo 1995)*[173] und 6. August 2001 *(Memo 2001)*[174] wurde die Möglichkeit eines Informationsaustausches zwischen dem Geheimdienst- und dem Strafverfolgungssektor beidseitig reduziert.[175] Eine Übermittlung von Geheimdienstinformationen war lediglich nach dem sogenannten *reasonable indication*-Standard zulässig. Voraussetzung war danach das Vorliegen objektiv bestimmter Tatsachen, die nach vernünftigen Maßstäben auf eine schwere Straftat hinweisen.[176] Zudem bedurfte die Informationsweitergabe teilweise einer vorherigen Einbeziehung des *Office of Intelligence Policy and Review* (OIPR)[177] sowie in Zweifelsfragen des Justizministers.[178] Eine Anfrage des Strafverfolgungssektors an die Dienste unterlag ebenfalls hohen Anforderungen und bedurfte einer exakten Beschreibung und Begründung sowie der Genehmigung durch die interne Sicherheitsabteilung der Strafrechtsdivision des Justizministeriums.[179] Diese Bestimmungen wurden zusätzlich durch ein zwischengeschaltetes Überprüfungsverfahren *(screening)* ergänzt, das die Weitergabe auf relevante Erkenntnisse limitierte. Diese Vorgaben führten dazu, dass Ermittlungen gegen das gleiche Zielobjekt zum Teil in unterschiedlichen Ermittlungseinheiten des FBI durchgeführt werden.[180] Die erheblichen Behinderungen beim Informationsaustausch zwischen den Strafverfolgungs- und den Geheimdienstbehörden wurden als Preis für die im Gegenzug umfassenden Ermächtigungen des FISA akzeptiert.[181]

Diese Grenzziehung wurde nach den Ereignissen vom 11. September 2001 durch die Aufhebung der *wall* und eine Erweiterung des Informationsaustauschs aufgege-

---

171 So etwa in *United States v. Belfield* 692 F.2d 141, 149 (D.C. Cir. 1982*); United States v. Cavanagh* 807 F.2d 787, 791 (9th Cir. 1987). Vgl. zudem zum Bereich der *foreign intelligence Birkenstock* Geo. L. J. (80) 1992, S. 863.

172 Vgl. *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 229.

173 Vgl. http://epic.org/privacy/terrorism/fisa/ag_1995_mem.html [Stand: 1.5.2012].

174 Vgl. http://epic.org/privacy/terrorism/fisa/08_2002_mem.html [Stand: 1.5.2012].

175 Vgl insgesamt *Kris/Wilson,* § 10:8 sowie § 10:7, S. 369f; *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 228; *Vervaele,* Utrecht L. Rev. (1) 2005, S. 6.

176 Vgl. Memo 2001 unter Punkt 1: "specific facts or circumstances indicating a past, current, or impending violation. There must be an objective, factual basis for initiating the investigation; a mere hunch is insufficient." Vgl. *Vervaele,* Utrecht L. Rev. (1) 2005, S. 6.

177 Hierbei handelt es sich um eine Abteilung des Justizministeriums.

178 Memo 2001 unter Punkt 1; vgl. *Chiarella/Newton,* Army Law. (25) 1997, S. 28; *Roach*, Challenges, S. 41; *Vervaele,* Utrecht L. Rev. (1) 2005, S. 6.

179 Vgl. *Vervaele,* Utrecht L. Rev. (1) 2005, S. 6.

180 Vgl. hierzu *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 4.

181 Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 4; *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 229.

ben.[182] Die als Reaktion auf die Anschläge einberufene *9/11-Commission* deckte erhebliche Mängel beim Informationsaustausch zwischen den *intelligence* und *non-intelligence*-Einheiten des FBI sowie in der Zusammenarbeit mit den anderen Diensten auf.[183] Insbesondere die Aufteilung zwischen *domestic* und *foreign intelligence* erschien für eine Bekämpfung des innerhalb der USA agierenden internationalen Terrorismus nicht geeignet.[184] In diesem Zusammenhang wurde die *wall* als erhebliches Defizit der Terrorabwehr kritisiert.[185] Als Reaktion wurde der USA PATRIOT Act 2001 erlassen, der den Informationsaustausch zwischen den verschiedenen Sicherheitsbehörden verbessern sollte.[186] Das bisherige *need to know*-Prinzip wurde zugunsten des *need to share*-Gedankens aufgegeben. Terrorrelevante Erkenntnisse waren nunmehr unabhängig vom Erhebungsort und der erhebenden Behörde austauschbar.[187] Der *primary purpose*-Test und damit die Sonderstellung der FII wurde durch eine Wortlautänderung des FISA von „the purpose" zu „a significant purpose" aufgegeben.[188]

Die mit den Reformen verbundenen Gesetzesänderungen waren jedoch zunächst mit Unsicherheiten behaftet, die vor allem die Reichweite des neu geschaffenen *significant purpose*-Standards im FISA betrafen. Im erläuternden Memorandum vom 6. März 2002 *(Memo 2002)*[189] ging der damalige *Attorney General Ashcroft* sowohl von einem vollumfänglichen Einsatz des FISA zu Strafverfolgungszwecken als auch einer vollumfänglichen Austauschbarkeit von FISA-Erkenntnissen aus.[190]

Diese Interpretation wurde vom FISCR *(FISC of Review)* als dem Revisionsgericht zum FISC nur teilweise aufrechterhalten. Zwar bestätigte der FISCR die Abschaffung des *primary purpose*-Tests und der *wall,* gleichzeitig betonte er

---

182 Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 5; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 419f; *Vervaele,* Utrecht L. Rev. (1) 2005, S. 8.

183 Vgl. *Roach*, Challenges, S. 41.

184 Vgl. *M. McCarthy,* Harv. J. Leg. (39) 2002, S. 442.

185 Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 5, sowie die Berichte der 9/11 Commission unter http://www.gpoaccess.gov/911/pdf/fullreport.pdf [Stand: 1.5.2012].

186 Vertiefend *Chesney,* in: Commission of Inquiry, S. 86.

187 Vgl. *M. McCarthy,* Harv. J. Leg. (39) 2002, S. 442. Für den Informationsfluss aus dem Geheimdienst- in den Strafverfolgungssektor vgl. USA PATRIOT Act sec. 504.

188 Siehe 50 U.S.C. §§ 1804(a)(6)(B) und 1823(a)(6)(B); vgl. *Becker,* RIDP/IRPL 2009, S. 348; *Grunwald,* S. 88; *Kris/Wilson,* § 10:10, S. 374ff; *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 230. Der Vorschlag, den Wortlaut von „the purpose" durch „a purpose" zu ändern, wurde nicht angenommen; vgl. *Standler*, S. 17f.

189 Zu finden unter http://epic.org/privacy/terrorism/fisa/ag_mem_03_2002.html [Stand: 1.5.2012].

190 Vgl. Memo 2002 unter Punkt A: "The Criminal Division and OIPR shall have access to all information developed in full field FI and FCI investigations except as limited by orders issued by the Foreign Intelligence Surveillance Court", vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 153; *Vervaele,* Utrecht L. Rev. (1) 2005, S. 9f. Etwas anderes galt nur, wenn der FISC ausdrücklich widersprach.

jedoch, dass hierzu die Änderungen durch den USA PATRIOT Act nicht erforderlich gewesen wären.[191] Der FISCR erklärte vielmehr, dass die jahrelang favorisierte formale Aufteilung auf einer fehlerhaften Interpretation durch die Gerichte beruhte und im FISA selbst niemals angelegt gewesen sei.[192] Weiterhin stellte das Gericht fest, dass das Vorliegen eines Strafverdachts nicht die Wahrung nationaler Sicherheitsinteressen hindere, sondern die Strafverfolgungsbehörden durchaus mehrere Zwecke verfolgen könnten.[193] Der auf die Auslandsaufklärung ausgerichtete FISA könne daher zu Strafverfolgungszwecken eingesetzt werden, solange die Strafverfolgung nicht den einzigen Zweck *(sole purpose)* der Informationserhebung darstellt.[194] Von einer Unzulässigkeit sei jedoch dann auszugehen, wenn die FISA-Maßnahmen von vorneherein ausschließlich auf die Strafverfolgung gerichtet seien. Dies gelte selbst dann, wenn dieser *sole purpose* sogenannte *foreign intelligence crimes* betraf.[195] In diesem Punkt widersprach der FISCR damit dem Memo 2002, das von einer schrankenlosen Einsatzmöglichkeit des FISA zu Strafverfolgungszwecken ausgegangen war.

Bei genauerer Betrachtung engt die FISCR-Rechtsprechung den Ansatz des Memo 2002 letztlich nur geringfügig ein. Die Anforderungen des gesetzlich vorgesehenen *significant purpose* sind bereits erfüllt, wenn der Zweck nicht allein die Strafverfolgung ist.[196] Diese darf den primären, nicht aber den einzigen Zweck der Überwachung darstellen. Eine Grenzüberschreitung ist erst erreicht, wenn jegliche Beziehung zwischen der FISA-Überwachung und den nachrichtendienstlichen

---

191 Vgl. *In re Sealed Case*, 310 F.3d 717, 722 (FISCR 2002). Damit widerspricht der FISCR dem FISC, der diese Änderung zuvor beanstandet hatte, vgl. *Arzt,* in: Graulich/Simon, S. 259; *Becker,* RIDP/IRPL 2009, S. 346f; *Kris/Wilson,* § 10:12, S. 381; *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 235f; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 420; *Vervaele,* Utrecht L. Rev. (1) 2005, S. 8f, 11.

192 Vgl. *In re Sealed Case*, 310 F.3d 717, 727: "In sum, we think that the FISA as passed by Congress in 1978 clearly did not preclude or limit the government's use or proposed use of foreign intelligence information".

193 Vgl. *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 236.

194 *In re Sealed Case*, 310 F.3d, 717, 735 heißt es: "if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct – even foreign intelligence crimes – to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied"; vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 152f; *Kris/Wilson,* § 10:14, S. 384.

195 Vgl. *In re Sealed Case*, 310 F.3d, 717, 735, sowie *Grunwald,* S. 125; *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 152; *Kris/Wilson,* § 10:14, S. 384. *Foreign intelligence crimes* sind Delikte, die mit Bedrohungen feindlicher ausländischer Staaten und Organisationen in Zusammenhang stehen, also sämtliche Aktivitäten, auf die im Rahmen des FISA in 50 U.S.C. § 1801(a)–(e) Bezug genommen wird. Beispiele hierfür sind etwa Spionage, der internationale Terrorismus, Sabotage sowie damit untrennbar verbundene Delikte, wie z.B. die finanzielle oder praktische Unterstützung des Terrorismus.

196 Vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 153; *Kris/Wilson,* § 10:14, S. 384.

Aufgaben beziehungsweise der Auslandsaufklärung fehlt.[197] Es lässt sich damit festhalten, dass die Reformen nach 2001 zu einem Wegfall der *wall* und einer weitgehenden Integration des Geheimdienstsektors in die restliche Sicherheitsarchitektur führten. Die Korrekturen durch den FISCR führten nur zu einer geringfügigen Beschränkung des Informationsaustausches. Die Sonderstellung der FII sowie die Trennung zwischen geheimdienstlicher und polizeilicher Tätigkeit wurden weitgehend aufgehoben.[198]

Diese Angleichung wird vor allem am FBI deutlich, für das mit den Mukasey Guidelines von 2008, unabhängig von der Zielsetzung der Ermittlungsmaßnahme, einheitliche Standards für Ermittlungen im Inland existieren.[199] Durch den Verzicht auf den *primary purpose*-Test wurden zudem die Erhebungs- und Austauschmöglichkeiten im Bereich der Inlandsaufklärung massiv ausgeweitet.[200]

Die in der *Mayfield*-Entscheidung[201] bezweifelte Verfassungsmäßigkeit des *USA PATRIOT Act* konnte diese Tendenz nicht korrigieren, da in den Rechtsmittelentscheidungen aus den Jahren 2009[202] und 2010[203] die für eine Verletzung des vierten Verfassungszusatzes erforderliche individuelle Betroffenheit *(standing)* verneint wurde. Trotz dieser obergerichtlichen Anerkennung wird die Abschaffung des *primary purpose*-Tests durch den USA PATRIOT Act von 2001 weiterhin heftig diskutiert.[204] Die Befürworter der Reform verweisen auf den klarstellenden Charakter der Änderungen, durch den eine bis dato fehlerhafte Interpretation des FISA berichtigt werde.[205] Die Trennung strafrechtlicher und geheimdienstlicher Fragestellungen sei im FISA zu keinem Zeitpunkt angelegt gewesen. Der *primary purpose*-Test basiere vielmehr auf der vor Erlass des FISA ergangenen *Truong*-Entscheidung und hätte den Informationsaustausch nur unnötig behindert.[206] Zudem verkenne die Gegenansicht die strafrechtliche Relevanz terroristischer Akte.

---

197 Vgl. *Arzt,* in: Graulich/Simon, S. 259. Hiervon sei etwa bei gewöhnlichen Straftaten auszugehen.

198 So *Grunwald,* S. 88; *Hulnick,* IJIC (22) 2009, S. 575; *Jäger/Daun,* in: Borchert, S. 69.

199 Vgl. *Berman*, S. 7; *Johnson,* I/S: J.L. & Pol'y for Info. Soc'y (5:3) 2010, S. 439.

200 Zum Teil wird sogar die Einführung eines eigenständigen Inlandsgeheimdienstes gefordert, vgl. *Cowan*, S. 14ff; *Hulnick,* IJIC (22) 2009, S. 569ff; *Posner,* S. 67ff; *Rascoff,* S. Cal. L. Rev. (83) 2010, S. 575ff; *Treverton,* Reorganizing, S. 85ff. Hierdurch sollen die Möglichkeiten der Inlandsaufklärung erweitert und neue Erkenntnisquellen geschaffen werden.

201 *Mayfield v. United States*, 504 F. Supp. 2d 1023, 1036ff, 1042f (D. Or. 2007).

202 *Mayfield v. United States*, 588 F.3d 1252 (9th Cir. 2009).

203 *Mayfield v. United States*, 599 F.3d 964 (9th Cir. 2010).

204 Vgl. zur Abschaffung insgesamt *Grunwald,* S. 88ff.

205 Vgl. *A. McCarthy*.

206 Zur *wall* als erhebliches Hemmnis *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 251.

Diese Argumentation versuchen die Kritiker in mehrerlei Hinsicht zu entkräften. Als ersten Aspekt führen sie an, dass die Geltung des *primary purpose*-Tests selbst nach der Schaffung des FISA jahrelang von den Gerichten aufrechterhalten und bestätigt wurde.[207] Darüber hinaus könne von einer Trennung strafrechtlicher und geheimdienstlicher Aspekte nicht die Rede sein, da die Verfolgung strafrechtlicher Zwecke auch in der ursprünglichen Fassung des FISA nicht zur Beendigung der Ermittlungen geführt hätte. Durch den *primary purpose*-Test sei vielmehr eine Umgehung strafrechtlicher Standards verhindert worden, indem ab Überwiegen einer primär strafrechtlichen Zwecksetzung zusätzlich ein *warrant* i.S.d. vierten Verfassungszusatzes eingeholt werden musste. Als dritten Punkt führen sie den auch zum damaligen Zeitpunkt möglichen – wenn auch kontrollierten – Informationsaustausch nach dem FISA an. Dies belege, dass die strafrechtliche Relevanz terroristischer Akte gerade nicht verkannt werde. Ausschlaggebend für die tragischen Informationsdefizite von 2001 seien insofern nicht gesetzliche, sondern bürokratische Hindernisse gewesen. In diesem Zusammenhang habe vor allem das zwischen FBI und CIA bestehende gegenseitige Misstrauen eine wichtige Rolle gespielt.[208] Schließlich werde dem FISA ohne die Bindung an den „primären Zweck" der Auslandsaufklärung die bisherige Grundlage für die Freistellung von den Vorgaben des vierten Verfassungszusatzes entzogen.[209] Bislang sei die Freistellung von der *probable cause*-Schwelle unter der sogenannten *special needs exception* gerechtfertigt gewesen. Hierzu musste die staatliche Maßnahme einem von Strafverfolgungszwecken abtrennbaren Sicherheits- oder Schutzbedürfnis dienen.[210] Diese Unterscheidung sei im Rahmen des FISA seit dem Verzicht auf den *primary purpose*-Test gerade nicht mehr möglich. Der FISA in seiner jetzigen Fassung sei daher verfassungswidrig.

Die im Jahr 2001 angestoßene Integration des Geheimdienstsektors setzte sich in den Folgejahren fort und schlug sich in einem verstärkten Datenaustausch sowie dem Aufbau verschiedener Informationsverbunde nieder. Ausgehend von den bereits bestehenden Änderungen wurde versucht den Informationsaustausch durch eine strategische Neuausrichtung und Schaffung neuer Institutionen weiter zu optimieren. In institutioneller Hinsicht wurde mit dem *Homeland Security Act 2002* das Heimatschutzministerium (DHS) als eine Koordinierungsstelle zum Schutz der amerikanischen Bevölkerung vor terroristischen und anderen Bedrohungen des amerikanischen Staatsgebietes geschaffen, das sämtliche Akteure des Geheimdienstsektors unter einem Dach zusammenführt.[211] In strategischer Hinsicht kam es

---

[207] Vgl. *Standler*, S. 23.

[208] So *Cole*.

[209] Vgl. *Cole*; *Grunwald,* S. 102ff; *Hardin,* Geo. Wash. L. Rev. (71) 2003, S. 334, 341; *Standler*, S. 17.

[210] Vgl. *Kris/Wilson,* § 11:14, S. 421; *Whitney*, S. 135ff.

[211] Vgl. *Hulnick,* IJIC (22) 2009, S. 575.

durch verschiedene Gesetze, Anordnungen und Empfehlungen zum Aufbau einer sogenannten *information sharing environment* (ISE), die den Austausch terrorrelevanter Informationen zwischen den Geheimdiensten, Strafverfolgungsbehörden und sonstigen Einheiten auf Bundes- und Staatenebene erleichtern sollte.[212] Als wesentliches Element dieser ISE wurden der DNI und das ihm zuarbeitende *National Counterterrorism Center* (NCTC)[213] geschaffen. Der DNI koordiniert und optimiert unter anderem den Informationsaustausch zwischen den verschiedenen Geheimdiensten.[214] Das NCTC führt in einer zentralen Datenbank sämtliche terrorrelevanten Erkenntnisse der verschiedenen Bundesbehörden zusammen und stellt deren Analyse den verschiedenen Behörden sowie dem Präsidenten in täglichen Berichten zur Verfügung.[215] Daneben wurden mit den *Joint Terrorism Task Forces* (JTTF) und den *Intelligence Fusion Centers* verschiedene Kooperationsformen geschaffen. Bei den JTTF handelt es sich um Zusammenschlüsse von Mitgliedern des FBI und lokaler Strafverfolgungsbehörden, mit deren Hilfe die zwischenbehördliche Koordination im Kampf gegen den Terrorismus optimiert und der Informationsfluss zwischen den Behörden auf Bundes- und Einzelstaatenebene gestärkt werden soll.[216] Bei den seit 2003 entstehenden *Intelligence Fusion Centers* handelt es sich um lose Zusammenschlüsse mehrerer Behörden, die durch einen Informationsaustausch sowohl die Kriminalitäts- als auch die Terrorbekämpfung verbessern sollen.[217] Darüber hinaus wurden bundesweite Datenbanken geschaffen, auf welche die einzelnen Kooperationsformen zurückgreifen können. Hierzu zählt etwa die *Nationwide Suspicious Activity Reporting Initiative*, in welche die Polizeibehörden bundesweit Daten über verdächtiges Verhaltens einstellen kön-

---

[212] Vgl. den National Criminal Intelligence Sharing Plan (NCISP), den Intelligence Reform and Terrorism Prevention Act (IRTPA) und die E.O. 13356 bzw. 13388 aus den Jahren 2004 und 2005 mit dem Titel "Strengthening the Sharing of Terrorism Information to Protect Americans"; vgl. auch *Best,* CRS 2011, S. 6; *Bjelopera,* CRS 2011, S. 1; *Hörauf,* S. 317; *Swire,* Vill. L. Rev. (51) 2006, S. 953.

[213] Vgl. *Hörauf,* S. 316f, sowie den offiziellen Internetauftritt unter http://www.nctc.gov/about_us/what_we_do.html [Stand: 1.5.2012].

[214] Daneben wird er als *principal adviser* beratend für den Präsidenten, den *National Security Council* (NSC) und den *Homeland Security Council* (HSC) tätig und beaufsichtigt den Geheimdienstsektor, vgl. ODNI Guide 2009, S. 8, 22; ODNI zur IC 2009, S. 1; vgl. auch E.O. 12333 von 2008 unter Punkt 1.3. sowie *Becker,* RIDP/IRPL 2009, S. 349; *Swire,* Vill. L. Rev. (51) 2006, S. 953. Der DNI ersetzt in dieser Funktion damit den bisher mit dieser Aufgabe betrauten Leiter der CIA, den *Director of Central Intelligence* (DCI), dem bis dahin eine Doppelfunktion zukam.

[215] Vgl. hierzu den offiziellen Internetauftritt des NCTC unter http://www.nctc.gov/about_us/about_nctc.html [Stand: 1.5.2012] sowie *Jäger/Daun,* in: Borchert, S. 70f.

[216] Vgl. *Rozen,* in: Markle Foundation, S. 118.

[217] Momentan existieren ca. 70 *Intelligence Fusion Centers*; vgl. die offiziellen Angaben der Regierung unter http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181 [Stand: 1.5.2012] sowie *Bjelopera,* CRS 2011, S. 1.

nen.[218] Die zunehmende Vernetzung der verschiedenen Sicherheitsbereiche setzt sich bis heute fort und kommt in verschiedenen Programmen wie der *National Intelligence Strategy* von 2009 (NIS),[219] der *National Security Strategy* von 2010 (NSS)[220] und der *National Intelligence Sharing Strategy* des FBI von 2011 (NISS)[221] zum Ausdruck. Diese fordern jeweils eine bessere Integration bestehender Ermittlungskapazitäten sowie eine Optimierung des Informationsaustauschs zur Verhinderung terroristischer Anschläge.

3. Zwischenergebnis

Die im Ausgangspunkt bestehende Differenzierung zwischen geheimdienstlichen und strafrechtlichen Ermittlungen wurde in den USA weitgehend aufgegeben und durch eine Aufteilung in strafrechtliche und auslandsbezogene Ermittlungen ersetzt. Formal wird weiterhin zwischen geheimdienstlichen Maßnahmen im Aus- und Inland sowie in Bezug auf die Inlandsüberwachung zwischen rein inländischen Sachverhalten (DII) und solchen mit Auslandsbezug (FII) unterschieden. Der Bereich der DII folgt dabei den strafrechtlichen Regeln, wohingegen sich FII nach den Vorgaben des FISA richten. Seit Abschaffung des *primary purpose*-Tests können diese Unterschiede bei der praktischen Rechtsanwendung jedoch leicht umgangen werden. Die ehemals formale Trennung hat mit der Öffnung des FISA an Bedeutung verloren. Verbleibende Unterschiede werden durch die wachsende Zahl an Informationsverbünden zusätzlich eingeebnet, sodass ein Informationsaustausch weitgehend unabhängig vom Erhebungskontext gestattet wird.[222]

B. Auswirkungen der Sicherheitsarchitektur auf die Informationsnutzung

1. Besonderheiten geheimdienstlicher Informationserhebung

Der nachfolgende Abschnitt widmet sich den Besonderheiten der geheimdienstlichen Informationserhebung im amerikanischen Kontext. Die charakteristischen Erhebungsstandards werden primär am Beispiel des FBI herausgearbeitet, welches im Rahmen der Inlandsaufklärung sowohl für rein inländische Sachverhalte als

---

218 Vgl. http://nsi.ncirc.gov/documents/NSI_Overview.pdf, S. 2 [Stand: 1.5.2012].

219 Vgl. http://www.dni.gov/reports/2009_NIS.pdf [Stand: 1.5.2012].

220 Vgl. www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf [Stand: 1.5.2012].

221 Vgl. http://www.fbi.gov/stats-services/publications/national-information-sharing-strategy-1/national-information-sharing-strategy-2011/view [Stand: 1.5.2012].

222 Vgl. *M. McCarthy,* Harv. J. Leg. (39) 2002, S. 442.

auch für Fragen mit Auslandsbezug zuständig ist.[223] Bei Bedarf wird ergänzend auf die besonderen Befugnisse der NSA und der CIA eingegangen. Maßgeblicher Anknüpfungspunkt der Untersuchung sind vor allem die Vorgaben der E.O. 12333, der Mukasey Guidelines von 2008 und der 50 U.S.C. §§ 401ff und 1801ff.

a) Geheimdienstliche Aufgaben und Aufklärungsrichtung

Die Aufgaben der Dienste wurden größtenteils bereits im Überblick über das amerikanische Geheimdienstwesen dargestellt, sodass sich die folgenden Ausführungen auf die Grundzüge beschränken. Im Mittelpunkt der geheimdienstlichen Aufgabenwahrnehmung steht die Sammlung und Aufbereitung von Informationen zu Fragen der nationalen Sicherheit, der Verteidigung, der auswärtigen Beziehungen sowie zum Schutz von Personen und Organisationen.[224] Die in diesem Zusammenhang erhobenen Erkenntnisse sollen eine Entscheidungsgrundlage für den Präsidenten, den *National Security Council* und den *Homeland Security Council* zu Fragen der Außen-, Verteidigungs-, Wirtschafts- und Sicherheitspolitik schaffen und Bedrohungen der nationalen Sicherheit verhindern helfen.[225] Um diesem Auftrag gerecht zu werden, ist den Diensten eine möglichst umfassende und frühzeitige Informationserhebung gestattet. Die geheimdienstlichen Ermittlungen können sich nicht nur auf kriminelle Verhaltensweisen, sondern auch auf *hostile activities* fremder Mächte, Organisationen, Personen oder Agenten sowie sonstige Informationen erstrecken.[226] Der Begriff der *hostile activities* ist umfassend zu verstehen, sie können sowohl in rechtswidrigem als auch legalem Verhalten bestehen.[227] Wird die Einleitung von Schutzmaßnahmen als nicht ausreichend erachtet, kann den Geheimdiensten unter der Leitung des Präsidenten zusätzlich die Durchführung aktiver Gegenmaßnahmen gestattet werden.

Der Fokus der geheimdienstlichen Aufklärung liegt trotz einer weitgehenden Integration des Geheimdienstwesens schwerpunktmäßig auf internationalen und auslandsbezogenen Bedrohungslagen sowie Aufklärungsmaßnahmen mit Auslandsbezug.[228] Derartige Maßnahmen unterliegen nicht in gleicher Weise wie Maßnahmen mit rein inländischem Bezug den Vorgaben des vierten Verfassungszusat-

---

[223] Vgl. Mukasey Guidelines 2008, II.A.1., II.B.1. Hierbei ist allerdings zu berücksichtigen, dass die Richtlinien zugleich für proaktives, polizeiliches Handeln des FBI gelten und sich damit auch auf die Verhinderung von Bundesstraftaten richten.

[224] Vgl. E.O. 12333 von 2008 unter Punkt 2.1, 2.3.

[225] Vgl. E.O. 12333 von 2008 unter Punkt 1.1. und 1.4 (a); Mukasey Guidelines 2008, S. 17, sowie *Chiarella/Newton,* Army Law. (25) 1997, S. 25; *Droste,* Nachrichtendienste, S. 88; *Lundberg,* in: Baldino, S. 59.

[226] Vgl. E.O. 12333 von 2008 unter Punkt 1.4 (b).

[227] Vgl. Mukasey Guidelines 2008, S. 9.

[228] Siehe E.O. 12333 von 2008 unter Punkt 1.1 (d)(1)–(3) sowie die Definition in 50 U.S.C. § 401a(5); vgl. zudem *Grunwald,* S. 75.

zes.[229] Geheimdienstliche Beobachtungsmaßnahmen sind zudem weniger auf das Verhalten einer Einzelperson, sondern vielmehr auf den Status oder die Zugehörigkeit einer Person zu einer bestimmten Gruppierung ausgerichtet.[230] Seit 2004 können durch die Einfügung des sogenannten *lone wolf amendment* neuerdings aber auch Einzelpersonen ohne konkrete Verbindungen zu einer terroristischen Organisation erfasst werden.[231] Als Voraussetzung für die Beobachtung eines *lone wolf* genügt ein Verdacht auf Beteiligung an Handlungen oder bloßen Vorbereitungsmaßnahmen des internationalen Terrorismus.[232] Diese Sonderregelung gilt nur für Personen, die weder die amerikanische Staatsbürgerschaft besitzen noch dauerhaft aufenthaltsberechtigt sind.[233] Die Einfügung des *lone wolf amendment* wird zum Teil heftig diskutiert.[234]

Die Befürworter der Neuregelung betonen, dass das *lone wolf amendment* lediglich eine bis dato bestehende Lücke schließe. Vor dieser Gesetzesänderung hätte der Staat trotz nachweislicher Beteiligung einer Person am internationalen Terrorismus keine Überwachung anordnen können.[235] Sie verweisen weiterhin auf die erforderliche Verbindung des *lone wolf* zu Akten des internationalen Terrorismus i.S.d. 50 U.S.C. § 1801(c), wodurch eine systemwidrige Anwendung des FISA auf rein inländische politische Gewalttaten verhindert werden könne.[236]

Demgegenüber wird nach Ansicht der Kritiker durch diese Regelung sowohl der Hintergrund als auch der Charakter des FISA verkannt. Das *lone wolf amendment* gestatte die Verfolgung von Einzeltätern unter den abgesenkten Voraussetzungen des FISA, obwohl es sich dabei grundsätzlich um eine originäre Aufgabe der Strafverfolgung handele.[237] Rechtfertigungsgrundlage der besonderen Ermittlungsstandards des FISA sei jedoch nicht nur der Auslandsbezug, sondern die Fokussierung auf ausländische Mächte und ihre Agenten.[238] Durch die Schaffung des FISA sollte

---

[229] Etwa weil der vierte Verfassungszusatz überhaupt nicht anwendbar ist oder weil der FISA die Erhebungsvoraussetzungen herabstuft.

[230] Vgl. *Baker,* Foreign Policy (97) Winter 1994–1995, S. 41.

[231] In 50 U.S.C. § 1801(b)(1)(C) wird daher die bisherige Definition von "agent of a foreign power" um eine neue Kategorie ergänzt, vgl. *Liu,* CRS 2011, S. 1. Eingefügt durch Section 6001 des Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458. Diese Regelung wurde im Mai 2011 bis zum 1. Juni 2015 verlängert, vgl. *Bradley,* Tul. L. Rev. (77) 2002, S. 489; *Grunwald,* S. 106f.

[232] 50 U.S.C. § 1801(b)(1)(C): "engages in international terrorism or activities in preparation therefore". Die Vorschrift zielt dementsprechend auf die erleichterte Erfassung von Personen, die sich selbstständig über das Internet radikalisieren.

[233] 50 U.S.C. §§ 1801(b), 1801(c).

[234] Eine eingehende Diskussion findet sich unter http://apps.americanbar.org/natsecurity/patriotdebates/lone-wolf-2#rebuttal [Stand: 1.5.2012].

[235] Vgl. *Woods*.

[236] So *Woods*.

[237] Vgl. *Bradley,* Tul. L. Rev. (77) 2002, S. 490.

[238] Vgl. *Hardin,* Geo. Wash. L. Rev. (71) 2003, S. 292; *Spaulding*.

gerade die bis dato sehr missbrauchsanfällige Inlandsaufklärung reguliert werden. Das im *lone wolf amendment* erfasste Handeln Einzelner reiche nicht aus, um die erforderliche auslandspolitische und militärische Relevanz zu begründen. Diese sei aber eine notwendige Bedingung für die Zulässigkeit einer FISA-Überwachungen.[239] Fehle es an dieser Voraussetzung, könne eine Überwachung nur unter Rückgriff auf strafprozessuale Ermächtigungsgrundlagen und den dort geltenden Schutzmechanismen erfolgen.

Die Überwachung rein inländischer Sachverhalte im Inland wird demgegenüber nicht als spezifisch geheimdienstliche Aufgabe anerkannt, sondern eher dem polizeilichen Aufgabenspektrum zugeordnet.[240] Umgekehrt wird die geheimdienstliche Beobachtung inländischer Gruppierungen mit Ausnahme der CIA den amerikanischen Geheimdiensten auch nicht ausdrücklich untersagt. Gerade die Mukasey Guidelines von 2008 ermächtigen das FBI umfassend zur Aufklärung und Verhütung von Bundesstraftaten und Bedrohungen der nationalen Sicherheit.[241] Eine Begrenzung auf auslandsspezifische Gefahren ist nicht enthalten, sodass das FBI ebenfalls zur geheimdienstlichen Überwachung rein inländischer Sachverhalte befugt ist.[242] Inwiefern die späteren Erkenntnisse allerdings als Beweismittel herangezogen werden können, bestimmt sich nach den klassischen Beweisregeln.

b) Geheimdienstliche Erhebungsbefugnisse

Bei der Erhebung von Geheimdienstinformationen können die Dienste auf verschiedene Ermittlungsmethoden zurückgreifen. Eine nicht abschließende Aufzählung findet sich in der E.O. 12333 von 2008 sowie speziell für das FBI in den Mukasey Guidelines 2008 unter Punkt II.A.4. und V.A.[243] Insbesondere dem FBI sind danach exemplarisch die Informationserhebung aus offen zugänglichen Quellen, Maßnahmen mit Einverständnis der betroffenen Person sowie der Zugang zu Unterlagen des Justizministeriums oder anderer staatlicher Behörden gestattet. Weiterhin zulässig sind die Befragung von Mitgliedern öffentlicher oder privater Einrichtungen,[244] die Durchführung verdeckter Ermittlungen,[245] die Durchsuchung von Personen und Räumen[246] sowie die akustische[247] und optische[248] Wohnraum-

---

239 Hierzu *Spaulding*.

240 Vgl. die Zielbeschreibung der E.O. 12333 von 2008 unter Punkt 1.1.

241 Mukasey Guidelines 2008, Introduction, A.

242 Vgl. hierzu *Grunwald,* S. 39f.

243 Erstere verweisen zum Teil auf die 50 U.S.C. §§ 401ff und 50 U.S.C. §§ 1801ff.

244 Mukasey Guidelines 2008, S. 20.

245 Siehe zu den *undercover operations* Mukasey Guidelines 2008, S. 31.

246 Siehe zu den *physical searches* 50 U.S.C. §§ 1821-1829, Mukasey Guidelines 2008, S. 32. Für strafrechtliche Ermittlungen vgl. FRCrimP Rule 41.

247 Siehe zum *eavesdropping* 50 U.S.C. § 1801(f).

überwachung. Schließlich kann mittels der sogenannten *subpoena*-Befugnisse die Herausgabe von Geschäftsunterlagen *(business records)* oder sonstigen Gegenständen *(any tangible things)* verlangt werden.[249] Im Bereich der elektronischen Überwachung sind die NSA und das FBI auf der Grundlage des FISA zur Erhebung von Telefonverbindungsdaten befugt. Diese können die angewählten Rufnummern und die Gesprächsdauer[250] sowie die bei einem bestimmten Anschluss eingehenden Anrufe[251] erfassen. Darüber hinaus dürfen die Dienste auf den Inhalt bestimmter Telekommunikationsvorgänge zugreifen.[252] Diese elektronischen Überwachungsmaßnahmen können bei Bedarf verschiedene oder unbestimmte Anschlüsse betreffen.[253] Eine solche sogenannte *roving surveillance* kommt zur Anwendung, wenn das Beobachtungssubjekt die Überwachung durch die Nutzung verschiedener Telefonanschlüsse verhindern will. Unter den Voraussetzungen einer *roving surveillance* kann die Überwachungsmaßnahme erweitert oder fortgeführt werden, ohne dass für jede einzelne Maßnahme eine gesonderte Anordnung erforderlich wäre. Zudem ist der FISA, entgegen seiner ursprünglichen Ausrichtung auf Ermittlungen im Inland, neuerdings auch auf Überwachungen von Personen außerhalb der USA anwendbar.[254] Schließlich wurde Anfang 2013 bekannt, dass die NSA unter dem Codenamen PRISM Daten von Internetnutzern bei Konzernen wie Google, Facebook, Yahoo, Apple oder Microsoft sammelt und diese bei Bedarf abruft.[255] Diese wenigen Beispiele verdeutlichen, dass die amerikanischen Geheimdienste damit umfassend sowohl offene als auch heimliche und technische Überwachungsmaßnahmen durchführen.

---

[248] Siehe zur *video surveillance* 50 U.S.C. §§ 1801(n). Die Ermächtigung wird durch eine weite Auslegung des Begriffs *contents* erreicht, der nicht auf die Erfassung verbaler Kommunikation begrenzt sei, vgl. *United States v. Koyomejian*, 970 F.2d 536, 540 (9th Cir. 1992).

[249] Siehe zur *administrative subpoena* 50 U.S.C. §§ 1861–1862; vgl. Mukasey Guidelines 2008, S. 31f. Für strafrechtliche Ermittlungen vgl. FRCrimP Rule 17(c)(1).

[250] Siehe zum *pen register trap* 50 U.S.C. §§ 1841–1846. Für strafrechtliche Ermittlungen vgl. 18 U.S.C. §§ 3121–3127.

[251] Siehe zu den *trap and trace devices* 50 U.S.C. §§ 1841–1846. Für strafrechtliche Ermittlungen vgl. 18 U.S.C. §§ 3121–3127.

[252] Siehe zur *electronic surveillance* oder *wiretap* 50 U.S.C. 1801–1812. Für strafrechtliche Ermittlungen vgl. 18 U.S.C. §§ 2510–2522.

[253] Vgl. 50 U.S.C. § 1804(a)(3)(B). Für strafrechtliche Ermittlungen vgl. 18 U.S.C. § 2518(3)(d); vgl. hierzu *Arzt,* in: Graulich/Simon, S. 261; *Hörauf,* S. 309; *Young,* Fordham L. Rev. (34) 2001, S. 1064.

[254] Vgl. 50 U.S.C. §§ 1881–1181g. Diese Vorschriften werden zum Teil durch militärische Ermächtigungsgrundlagen ergänzt, vgl. *Chiarella/Newton,* Army Law. (25) 1997, S. 31f.

[255] Vgl. die Berichte unter http://www.heise.de/newsticker/meldung/EU-macht-Druck-USA-versprechen-Auskunft-zu-PRISM-1888945.html; http://www.spiegel.de/netzwelt/netzpolitik/was-prism-in-wahrheit-ueber-google-facebook-und-co-sagt-a-905351.html [Stand: 15.6.13].

Eine vergleichende Betrachtung zeigt jedoch, dass die dargelegten Methoden in den meisten Fällen in gleicher Weise zu Polizei- und Strafverfolgungszwecken eingesetzt werden können.[256] Diese Parallelität wird bereits am Titel der Mukasey Guidelines von 2008 deutlich, der sich insgesamt auf inländische Operationen des FBI bezieht, ohne zwischen geheimdienstlichen und polizeilichen Aufgaben zu differenzieren. Diese Vereinheitlichung wurde bewusst eingeführt, um die Arbeit der ermittelnden Beamten zu erleichtern. Diese können nunmehr sämtliche Befugnisse ausüben, ohne zuvor die zum Teil schwierige Zuordnung zu einem speziellen Ermittlungsbereich vornehmen zu müssen.[257] Darüber hinaus ist die Einheitlichkeit der Ermittlungsbefugnisse vor allem für die Überwachung rein inländischer extremistischer Bestrebungen von Bedeutung, da der Kongress auf den Erlass einer Sonderermächtigung verzichtet hat. Während elektronische Überwachungsmaßnahmen im Bereich der FII auf den FISA gestützt werden können, ist für vergleichbare Maßnahmen im Bereich der DII ein Rückgriff auf die polizeilichen Ermächtigungen in 18 U.S.C. §§ 2510ff erforderlich.[258]

Daneben existieren Befugnisse, die ausschließlich den Geheimdiensten zur Verfügung stehen. Ein Beispiel ist die exklusiv der CIA eingeräumte Sonderbefugnis der *covert actions,* welche der CIA die aktive Beeinflussung politischer, wirtschaftlicher oder militärischer Bedingungen im Ausland gestatten.[259] Da diese Maßnahmen nicht primär der Informationserhebung dienen, können sie in der weiteren Untersuchung weitgehend außer Betracht bleiben. Eine wiederum relevante geheimdienstliche Sonderbefugnis bilden die sogenannten *National Security Letters* (NSL), welche die Erlangung persönlicher Daten gestatten.[260] Je nach Herausgabeverlangen können die NSL auf 18 U.S.C. § 2709, 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v oder 50 U.S.C. § 436 gestützt werden. Diese Ermäch-

---

[256] Vgl. insbesondere zum Bereich der elektronischen Überwachungsmaßnahmen *Smith/Howe,* in: Markle Foundation, S. 138ff.

[257] Mukasey Guidelines 2008, S. 7: "Hence, these Guidelines do not require that the FBI's information gathering activities be differentially labeled as 'criminal investigations,' 'national security investigations,' or 'foreign intelligence collections,' or that the categories of FBI personnel who carry out investigations be segregated from each other based on the subject areas in which they operate. Rather, all of the FBI's legal authorities are available for deployment in all cases to which they apply to protect the public from crimes and threats to the national security and to further the United States' foreign intelligence objectives. In many cases, a single investigation will be supportable as an exercise of a number of these authorities – i.e., as an investigation of a federal crime or crimes, as an investigation of a threat to the national security, and/or as a collection of foreign intelligence."

[258] Dies wird in den Mukasey Guidelines 2008, S. 32, sowie 18 U.S.C. § 2511(2)(f) klargestellt; vgl. auch *Grunwald,* S. 72, 76.

[259] Siehe 50 U.S.C. § 413b(e); E.O. 12333 von 2008 unter Punkt 1.7.(a)(4); vgl. *Hörauf,* S. 291. Das Wort *covert* bezieht sich auf die Geheimhaltung des Initiators, d.h. der Regierung, nicht der Operation selbst. Geheime Operationen werden mit dem Begriff *clandestine* beschrieben, vgl. *Kibbe,* Intelligence and National Security (22:1) 2007, S. 57.

[260] Vgl. Mukasey Guidelines 2008, S. 32. Nähere Informationen finden sich bei *Doyle,* CRS 2011.

tigungen treten neben die Vorschrift des FISA in 50 U.S.C. § 1861. Auffallend ist, dass keine der Vorschriften die Maßnahme selbst als *National Security Letter* benennt. Dessen ungeachtet hat sich diese Bezeichnung durchgesetzt. Mit der Versendung eines NSL kann, ähnlich der *subpoena*-Befugnisse, die Herausgabe von Finanz-, Telefon- und Emaildaten verlangt werden, ohne dass es einer richterlichen Anordnung bedarf. Formal handelt es sich bei einem NSL um einen schriftlichen Befehl an eine bestimmte Einrichtung, die erfragten Unterlagen auszuhändigen. Wie die Bezeichnung der Maßnahme bereits vermuten lässt, ist der Einsatz der NSLs auf Ermittlungen zum Schutz der nationalen Sicherheit ausgerichtet.[261] Die zu erhebenden Erkenntnisse müssen für die Bekämpfung oder Analyse des internationalen Terrorismus oder der Spionageabwehr von Relevanz sein. Eine Nutzung für rein strafrechtliche Ermittlungen scheidet daher in aller Regel aus.[262]

Ebenfalls von Interesse sind die der Geheimhaltung unterliegenden Ermittlungsmethoden der Geheimdienste. Ein Beispiel bilden etwa die dem FBI zur Verfügung stehenden *classified investigative technologies.* Hierbei handelt es sich um als geheimhaltungsbedürftig eingestufte Methoden, deren Anwendung dem FBI ausschließlich für Zwecke der nationalen Sicherheit und der Auslandsaufklärung und damit für die geheimdienstliche Informationsgewinnung erlaubt sind, nicht jedoch für die Aufklärung gewöhnlicher Bundestrafsachen.[263] Wie das FBI können auch andere Geheimdienste in der Regel auf zusätzliche Ermittlungsmethoden zurückgreifen, welche nicht zwingend in den Ermächtigungsgrundlagen benannt sein müssen. Für die CIA ergibt sich der nicht abschließende Charakter der normierten Ermittlungsbefugnisse bereits aus der vagen Formulierung in 50 U.S.C. § 403-4a(d)(1) sowie dem Verzicht auf eine gesetzliche oder gerichtliche Präzisierung der genannten Vorgaben. Schließlich kann der Präsident die Geheimdienste zu weiteren Erhebungsmaßnahmen ermächtigen. Grundlage dieser Befugnis bildet nach Ansicht der Exekutive die verfassungsrechtliche Stellung des Präsidenten als Oberster Befehlshaber aus dem zweiten Verfassungsartikel i.V.m. der Ermächtigung des Kongresses von 2001 im *Authorization for Use of Military Force* (AUMF).[264] Diese Regelungen bevollmächtigen den Präsidenten zur Durchführung aller notwendigen und geeigneten Maßnahmen gegen die Verantwortlichen und Unterstützer der Terroranschläge von 2001.[265] Die primär militärischen Mittel kön-

---

[261] Vgl. auch *Grunwald,* S. 213; *Kris/Wilson,* § 20:8.

[262] Einzig in 50 U.S.C. § 436 werden strafrechtliche Ermittlungen vom Anwendungsbereich erfasst.

[263] So Mukasey Guidelines 2008 unter Punkt V.B.2; vgl. *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 167.

[264] Vgl. *Gitenstein,* in: Wittes, S. 27. Vgl. zum AUMF Pub. L. No. 107-40, 115 Stat. 224ff (2001), abgedruckt bei *Grimmett,* CRS 2007, S. 6ff.

[265] Der Wortlaut spricht von der Befugnis "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such

nen sich nicht nur gegen Nationalstaaten, sondern auch gegen Organisationen oder Personen richten.[266] Ein Beispiel für die Wahrnehmung dieser Ermächtigung ist das Ende 2005 bekannt gewordene und kontrovers diskutierte Abhörprogramm der NSA, welches unter anderem als *NSA Surveillance Programm* beziehungsweise *Terrorist Surveillance Program* betitelt wurde.[267] In diesem Programm wurde die NSA zur elektronischen Überwachung im Inland abseits des Title III und des FISA ermächtigt.[268] Voraussetzung war der Aufenthalt eines Kommunikationsteilnehmers im Ausland sowie das Bestehen mutmaßlicher Verbindungen zur *Al Quaida*.[269] Nach erheblicher Kritik wurde das Programm 2007 ausgesetzt.[270]

Den amerikanischen Geheimdiensten stehen damit verschiedene Ermittlungsbefugnisse zur Verfügung. Der Vergleich zu Maßnahmen sonstiger Sicherheitsbehörden fällt dabei sehr uneinheitlich aus. Sofern die einzelnen Erhebungsmethoden gesetzlich fixiert wurden, finden sich kaum Aufklärungsbefugnisse, die ausschließlich geheimdienstlichen Zwecken vorbehalten sind. Allerdings sind die Befugnisse des amerikanischen Geheimdienstsektors keineswegs abschließend aufgelistet. 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.

c) Zeitlicher Rahmen geheimdienstlicher Ermittlungen

Der nächste Abschnitt widmet sich den zeitlichen Rahmenbedingungen geheimdienstlicher Ermittlungen. Die Darstellung orientiert sich hierbei an der im deutschen Landesbericht gewählten Reihenfolge. Es werden dementsprechend die polizeilichen und geheimdienstlichen Ermittlungsschwellen auf Gemeinsamkeiten und Unterschiede in Bezug auf Beginn und Ende der Ermittlungen untersucht. Die zeitlichen Rahmenbedingungen folgen hierbei speziellen Regeln, die eine klare Abgrenzung der einzelnen Kategorien erschweren.

---

organizations or persons". Vgl. *Arzt,* in: Graulich/Simon, S. 267; *Grimmett,* CRS 2007, S. 1.

266 Vgl. *Grimmett,* CRS 2007, S. 4.

267 Vgl. hierzu *Arzt,* in: Graulich/Simon, S. 267; *Bazan,* CRS 2008, S. 7; *Kris/Wilson,* § 15:1, S. 490ff.

268 Vgl. hierzu die Erklärung des Justizministeriums vom 27.1.2006 unter http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf [Stand: 1.5.2012]. Ebenso *Arzt,* in: Graulich/Simon, S. 267; *Kris/Wilson,* § 15, sowie die Rechtfertigung des *Attorney General* vom 19.1.2006 unter www.usdoj.gov/ag/readingroom/surveillance9.pdf [Stand: 1.5.2012].

269 Vgl. *Gitenstein,* in: Wittes, S. 27.

270 Vgl. hierzu *Hörauf,* S. 329.

aa) Beginn geheimdienstlicher Ermittlungen

Der Beginn geheimdienstlicher Ermittlungen ist gesetzlich nicht reguliert. Die maßgeblichen Schwellen orientieren sich vielmehr an den Vorgaben des vierten Verfassungszusatzes und verwaltungsinternen Richtlinien. Nachfolgend werden als Vergleichsmaßstab zunächst die Ermittlungsschwellen bei Maßnahmen zu Strafverfolgungszwecken dargestellt. Die hier gewonnenen Erkenntnisse werden für das Verständnis der geheimdienstlichen Ermittlungsschwellen nutzbar gemacht.

(1) Vergleichsmaßstab der strafrechtlichen Ermittlungen

Im amerikanischen Recht ist der Beginn staatlicher Ermittlungstätigkeit im Grundsatz weder durch eine konkrete Schwelle noch durch einen bestimmten Verdachtsgrad vorbestimmt.[271] Das FBI und die anderen Strafverfolgungs- und Polizeibehörden können nach eigenem Ermessen tätig werden, ohne dass hierfür ein bestimmter Verdachtsgrad erfüllt sein muss.[272] Umgekehrt löst das Vorliegen eines konkreten Verdachtes keine Ermittlungspflicht aus, da für die amerikanischen Polizei- und Strafverfolgungsbehörden das Opportunitätsprinzip gilt.[273] Das Greifen strafprozessualer Regelung und damit der zentrale Anknüpfungspunkt ist auf den Zeitpunkt eines formellen Arrests beziehungsweise die Einreichung der Anklageschrift i.S.d. *complaints* festgelegt.[274] Der Verzicht auf jegliche Ermittlungsschwellen gilt aber nicht für alle staatlichen Ermittlungstätigkeiten. Mit zunehmender Eingriffsintensität der Ermittlungsbefugnisse steigt regelmäßig die für den Eingriff erforderliche Verdachtsschwelle.[275]

Von zentraler Bedeutung ist die Grenze des vierten Verfassungszusatzes.[276] Dieser schützt den Einzelnen vor sogenannten *unreasonable searches and seizures* und damit vor ungerechtfertigten staatlichen Eingriffen.[277] Die Anforderungen des vierten Verfassungszusatzes wurden durch die Gerichte vielfach ausgebaut und sind dementsprechend äußerst komplex. Der durch *searches* und *seizure* eröffnete Anwendungsbereich erstreckt sich auf eine Vielzahl von staatlichen Zwangs- und Überwachungsmaßnahmen. Nach einhelliger Rechtsprechung erfasst der Begriff der *search* sämtliche staatlichen Maßnahmen, die in das erkennbare und nachvoll-

---

271 Vgl. *Grunwald,* S. 32.

272 Vgl. *Markwordt Skehan,* S. 101.

273 Vgl. *Goldstein*, Yale L.J. (69) 1960, S. 543ff.

274 Vgl. *Markwordt Skehan,* S. 101f.

275 Bei limitierten Eingriffen, wie z.B. der *temporary detention*, wird z.B. ein „angemessener Verdacht“ *(reasonable suspicion)* gefordert, vgl. *Markwordt Skehan,* S. 150.

276 Die dortigen Vorgaben gelten über die *due process*-Klausel des 14. Zusatzartikels ebenfalls für Behörden der Einzelstaaten.

277 Vgl. stellvertretend *Markwordt Skehan,* S. 129. Auf die weiteren Vorgaben des vierten Verfassungszusatzes wird an späterer Stelle eingegangen.

ziehbare Vertrauen des Einzelnen in den Schutz seiner Privatsphäre eingreifen.[278] *Search* umfasst beispielsweise Durchsuchungen von Personen, Sachen, Wohnungen und Dokumenten sowie das Abhören von Telefongesprächen als sogenanntes *wiretapping*. Der Begriff *seizure* erstreckt sich auf jede nicht unbedeutende Beeinträchtigung von Eigentums-, Besitz- und Freiheitsinteressen. Hiervon ist etwa auszugehen, wenn ein Regierungsvertreter den Besitz oder die Kontrolle über eine Sache oder Person erlangt.[279] Der Schutz des vierten Verfassungszusatzes wird dem Betroffenen allerdings nur bei einem berechtigten und von der Gesellschaft anerkannten Vertrauen in seine Privatsphäre zuteil, der sogenannten *reasonable expectation of privacy*.[280] Sind die genannten Anwendungsvoraussetzungen erfüllt, ist er vor ungerechtfertigten – *unreasonable* – staatlichen Eingriffen und Zugriffen auf sein Eigentum, seinen Besitz oder seine individuelle Freiheit geschützt. Dieser Schutzstandard gilt für alle US-Bürger und für alle zum Aufenthalt berechtigten Ausländer.[281]

Maßstab der Aktivitäten des Verfassungsschutzes ist die Angemessenheit des staatlichen Handelns *(reasonableness)*.[282] Diese bestimmt sich anhand einer Abwägung zwischen dem staatlichen Interesse an der Durchführung des Eingriffs und dem Bedürfnis des Bürgers nach Freiheit und Sicherheit.[283] Sofern keine speziellen Ausnahmen greifen, erfordert die Angemessenheit das Vorliegen einer gerichtlichen Bewilligung in Form eines *warrant.* Dieser muss sich wiederum auf einen hinreichenden Grund *(probable cause),* stützen können, um den Anforderungen der Angemessenheit zu genügen.[284] Mit Blick auf Maßnahmen der Strafverfolgung hat der *Supreme Court* einen solchen hinreichenden Grund bejaht, wenn im Zeitpunkt der Entscheidung ein umsichtiger Beobachter bei objektiver Betrachtung der Fakten und Umstände des konkreten Falls vom Vorliegen einer Straftat ausgeht.[285] Erforderlich ist ein auf gewisse Tatsachen gründender Verdacht strafbaren bezie-

---

278 Vgl. *Scheb/Scheb II,* S. 342.

279 Vgl. *Arzt,* in: Graulich/Simon, S. 248; *Scheb/Scheb II,* S. 342; *Smith/Howe,* in: Markle Foundation, S. 135. Allgemein zu den erfassten Schutzobjekten *United States v. Jacobsen*, 466 U.S. 109, 113f (S. Ct. 1984).

280 Vgl. *Markwordt Skehan,* S. 121f.

281 Vgl. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265, 271 (S. Ct. 1990); *Arzt,* in: Graulich/Simon, S. 246f; *Markwordt Skehan,* S. 116f. Es muss eine substantielle Verbindung existieren, die die Person als Teil der Bevölkerung erscheinen lässt.

282 Vgl. *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 155ff.

283 Vgl. *Camara v. Municipal Court*, 387 U.S. 523, 537 (1967): "determining reasonableness […] by balancing the need to search against the invasion which the search entails"; vgl. zudem *Kerr,* Tex. L. Rev. (88) 2010, S. 1673f; *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 155ff.

284 Vgl. *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 155ff; *Kerr,* Tex. L. Rev. (88) 2010, S. 1669; *Scheb/Scheb II,* S. 342.

285 Vgl. 18 U.S.C. § 3104 i.V.m. FRCrimP 41(c) sowie *Arzt,* in: Graulich/Simon, S. 248f; *Kris/Wilson,* § 11:5, S. 395. Vertiefend u.a. *Ornelas v. United States*, 517 U.S. 690, 696 (S. Ct. 1996); *Illinois v. Gates*, 462 U.S. 213, 238f (S. Ct. 1983).

hungsweise kriminellen Handelns.[286] Die *probable cause*-Schwelle bildet damit den zentralen zeitlichen Anknüpfungspunkt für *search and seizure*-Maßnahmen. Mangels Legalitätsprinzip fungiert diese Schwelle zwar nicht als Auslöser staatlicher Ermittlungstätigkeit, sie ist jedoch zumindest für die Rechtfertigung beziehungsweise Angemessenheit des Eingriffs ausschlaggebend.[287] Der Verdachtsgrad und die zu erfüllenden Anforderungen steigen mit zunehmender Eingriffsintensität.[288] Für den Einsatz elektronischer Überwachungsmaßnahmen nach 18 U.S.C. §§ 2510–2522 muss sich der besagte Verdacht beispielsweise auf eine der in § 2516 genannten Straftaten beziehen.[289] Der Nachweis eines im Einzelfall bestehenden berechtigen Schutzinteresses ist nicht erforderlich.[290] Die Durchführung eingriffsintensiver Maßnahmen zu Beweiserhebungszwecken ist damit durchaus an das Vorliegen einer bestimmten Ermittlungsschwelle gebunden.

(2) Ermittlungsschwellen der Geheimdienste

Die Erhebung von Geheimdienstinformationen unterliegt zunächst keinen besonderen Ermittlungsschwellen. Allerdings sind geheimdienstliche Ermittlungen im Inland als staatliches Handeln ebenfalls an die Verfassung gebunden. Geheimdienstliche Maßnahmen, die das Merkmal der *search* oder der *seizure* erfüllen, müssen sich daher im Grundsatz ebenfalls an den Anforderungen des vierten Verfassungszusatzes messen lassen.[291] Wie eingangs dargestellt, handelt es sich bei der *probable cause*-Schwelle jedoch nicht um einen starren Standard.[292] Die *reasonableness* als zentrale Vorgabe des vierten Verfassungszusatzes gestattet vielmehr die Berücksichtigung weiterer Interessen.[293] Nach den sogenannten *special needs exceptions* sind Ausnahmen gestattet, wenn die Maßnahmen nicht primär auf individuelles Verhalten abzielen, sondern spezielle, über die Zwecke der Strafverfolgung hinausgehende Sicherheitsinteressen verfolgen.[294] Diese reduzierten Anforderungen können das Erfordernis der richterlichen Anordnung, den Bezugspunkt des

---

286 Vgl. *Grunwald,* S. 45.

287 Vgl. *Markwordt Skehan,* S. 135.

288 Vgl. hierzu *Markwordt Skehan,* S. 135.

289 Vgl. *Arzt,* in: Graulich/Simon, S. 256; *Baker,* Foreign Policy (97) Winter 1994–1995, S. 41; *Zabel/Benjamin,* S. 79. Vertiefend zu den weiteren Voraussetzungen siehe 18 U.S.C. § 2518(3)(b),(c),(d) sowie *Kris/Wilson,* § 11:6.

290 So 18 U.S.C. § 2518(3)(a), vgl. *Arzt,* in: Graulich/Simon, S. 250.

291 Vgl. *Markwordt Skehan,* S. 117. Im Ausgangspunkt ähnlich *Kerr,* Tex. L. Rev. (88) 2010, S. 1675. Dies gilt nicht für Maßnahmen im Ausland.

292 Vgl. *Grunwald,* S. 44.

293 Vgl. *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 157.

294 *In re Sealed Case*, 310 F.3d 717, 745 (FISCR 2002) heißt es: "designed to serve the government's 'special needs, beyond the normal need for law enforcement'"; vgl. *Markwordt Skehan,* S. 144; *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 158.

Verdachts und die an den Verdacht zu stellende Bestimmtheit betreffen.[295] Die Einbeziehung öffentlicher Interessen kann damit unterschiedliche *probable cause*-Standards rechtfertigen. Dementsprechend kann bei geheimdienstlichen Ermittlungen die *reasonableness* früher gegeben sein als bei anderen Ermittlungszwecken.[296]

Die Gerichte haben eine Lockerung der *probable cause*-Schwelle für *foreign intelligence investigations* (FII) und *domestic intelligence investigations* (DII) grundsätzlich für möglich gehalten.[297] Die gerichtlich zugestandene Flexibilität der *probable cause*-Schwelle wurde allerdings nur im FISA und damit für den Bereich der FII gesetzlich fixiert. Die Rahmenbedingungen im Geheimdienstrecht unterscheiden folglich danach, ob es sich um eine rein inländische Überwachungsmaßnahme (DII) oder eine Maßnahme mit Auslandsbezug (FII) handelt.[298]

Für rein inländische Überwachungsmaßnahmen (DII) wurde auf die Schaffung eines dem FISA korrespondierenden Gesetzeswerkes verzichtet. Aus diesem Grund gilt die verfassungsrechtliche Vorgabe des hinreichenden Grundes zunächst in der Form, wie sie im vorgenannten Abschnitt für strafrechtliche Ermittlungen dargestellt wurde.[299] Auf untergesetzlicher Ebene werden die vagen Vorgaben der Rechtsprechung allerdings durch die Mukasey Guidelines von 2008 präzisiert, die in Bezug auf inländische Ermittlungen des FBI unterschiedliche Standards für Maßnahmen der *threat assessment* (Abschnitt II.A.), *preliminary investigations* (Abschnitt II.B.4.a) und *full investigations* (Abschnitt II.B.4.b.) aufstellen.[300] Mittels Maßnahmen der *threat assessment* wird in der Regel abgeklärt, ob aus Gründen der nationalen Sicherheit weitere Ermittlungen erforderlich

---

[295] Vgl. zu den unterschiedlichen *warrant*-Standards *Kerr,* Tex. L. Rev. (88) 2010, S. 1676.

[296] Vgl. für den Bereich der DII die *Keith*-Entscheidung 407 U.S. 297, 322 (1972): "the focus of domestic surveillance may be less precise than that directed against more conventional types of crime. […] Different standards may be compatible with the Fourth Amendment"; vgl. zudem *Chiarella/Newton,* Army Law. (25) 1997, S. 29 Fn. 29; *Doyle*, CRS 2006, S. 1; *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 157; *Kerr,* Tex. L. Rev. (88) 2010, S. 1676; *Liu,* CRS 2011, S. 1. Vgl. allgemein zur Abwägung mit den staatlichen Interessen *Samson v. California*, 547 U.S. 843, 848 (2006) ("Whether a search is reasonable 'is determined by […] the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests'"); ähnlich *Illinois v. Lidster*, 540 U.S. 419, 427 (2004).

[297] Vgl. ebenda 407 U.S. 297, 322f (1972) sowie *Birkenstock,* Geo. L. J. (80) 1992, S. 866; *Grunwald,* S. 72.

[298] Vgl. zur Abgrenzung anhand des 4. Verfassungszusatzes *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 159.

[299] Zur grundsätzlichen Geltung der verfassungsrechtlichen Vorgaben im Rahmen geheimdienstlicher Ermittlungen vgl. *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 156.

[300] Die Richtlinie stellt nur freiwillige, interne Selbstbeschränkungen auf, ohne Rechte Außenstehender zu begründen, vgl. Mukasey Guidelines 2008, Punkt I.D.2. Dessen ungeachtet können aus der Richtlinie gewisse Grundstandards abgeleitet werden.

sind.[301] Ihr Einsatz erfordert weder das Vorliegen tatsächlicher Hinweise noch sonstiger Ermittlungsschwellen.[302] Aufgrund dieser fehlenden Begrenzungen sollen die gestatteten Methoden grundsätzlich von "relatively low intrusiveness" und damit zumindest theoretisch von geringer Eingriffsintensität sein.[303] Die Untersuchung der eingeräumten Ermittlungsbefugnisse in Abschnitt II.A.4. zeigt jedoch, dass neben der Nutzung öffentlich zugänglicher Quellen (II.A.4.a) auch der Einsatz menschlicher Quellen und Informanten (II.A.4.e) gestattet wird.[304] Auf der Grundlage der *threat assessment* ist damit beispielsweise die Infiltration einer Moschee durch Ermittlungspersonen unter Verheimlichung der wahren Identität möglich. Ein Schutz über den vierten Verfassungszusatz scheidet aus, da dessen Anwendbarkeit an der fehlenden *reasonable expectation of privacy* scheitert. Nach Ansicht der Rechtsprechung besteht kein Vertrauensschutz dahingehend, dass Personen dem Betroffenen mit ihrer wahren Identität gegenübertreten.[305] Dies verdeutlicht, dass Maßnahmen der *threat assessment* durchaus eine gewisse Eingriffsintensität erreichen können.[306] Auf einer zweiten Ebene folgen die *preliminary investigations*. Diese erfordern Indizien oder Anhaltspunkte, die auf eine Bedrohung für die nationale Sicherheit hinweisen.[307] Ist diese Schwelle erreicht, darf eine Vielzahl an Ermittlungsmethoden durchgeführt werden.[308] Es werden unter anderem *undercover operations* (V.A.7.) sowie der Zugriff auf Dokumente von Telekommunikationsanbietern und sonstigen Dienstleistern (V.A.8., V.A.9.) gestattet. Auf einer letzten Stufe folgen *full investigations*, auf deren Grundlage elektronische Überwachungsmaßnahmen, Durchsuchungen i.S.d. FRCrimP 41 oder Maßnahmen nach dem FISA durchgeführt werden können. Erforderlich ist eine Tatsachenbasis, die vernünftigerweise auf eine Gefährdung der nationalen Sicherheit hinweist.[309] In allen drei Ermittlungsbereichen kann das FBI damit eingriffsintensive Maßnahmen einsetzen, ohne diese zugleich an gesteigerte Verdachtsanforderungen zu knüpfen.

Im Bereich der *foreign intelligence investigations* wird durch die Regelungen des FISA eine zusätzliche Modifikation beziehungsweise Absenkung der Ermittlungs-

---

301 Mukasey Guidelines 2008, Punkt II.A.1.

302 Vgl. *Berman*, S. 22; *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 165.

303 Mukasey Guidelines 2008, Punkt II. auf S. 17.

304 Kritisch hierzu *Berman*, S. 22.

305 Vgl. *United States v. White*, 401 U.S. 745, 751 (7th Cir.1971).

306 *Berman*, S. 22, spricht von "highly intrusive investigative techniques".

307 Nach den Mukasey Guidelines 2008, II.B.4.a.i. i.V.m. II.B.3.a–b können *preliminary investigations* durchgeführt werden "on the basis of information or an allegation indicating" "a federal crime or a threat to the national security"; vgl. *Berman*, S. 21f.

308 Vgl. Mukasey Guidelines 2008, II.B.4.a.iii., V.A.11.–13.

309 Die Mukasey Guidelines 2008 fordern unter Punkt II.B.4.b.i. i.V.m. § II.B.3a.–c. eine "articulable factual basis" und "reasonable indications"; vgl. *Berman*, S. 22.

schwellen erreicht.[310] Wesentliches Merkmal der im Rahmen des FISA geltenden Ermittlungsschwellen ist der von strafrechtlichen Ermittlungen abweichende Bezugspunkt. Erforderlich ist nicht der Verdacht einer Straftat, sondern das Vorliegen eines tauglichen Beobachtungsobjektes. Von einem solchen ist auszugehen, wenn sich die Beobachtung gegen eine ausländische Macht oder den Agenten einer ausländischen Macht richtet.[311] Das Merkmal einer ausländischen Macht erfüllen unter anderem ausländische Regierungen oder Regierungseinheiten sowie überwiegend aus *Non-U.S. Persons* zusammengesetzte politische Organisationen.[312] Als Agent einer ausländischen Macht werden wiederum *U.S. Persons* als auch *Non-U.S. Persons* eingestuft, die wissentlich geheimdienstliche Erkenntnisse sammeln und dadurch Delikte des Bundesstrafrechts verletzen oder verletzen könnten.[313] Daneben führt die bewusste Beteiligung an Sabotagehandlungen oder Aktivitäten des internationalen Terrorismus, die Einreise unter einer falschen Identität sowie die Unterstützung oder Abrede zu solchen Handlungen zu einer Einstufung als Agent einer fremden Macht.[314] Durch die Bezugnahme auf Delikte des Bundesstrafrechts scheint der FISA zunächst an eine dem Strafverfahrensrecht entlehnte Schwelle anzuknüpfen. Bei genauerer Betrachtung fällt allerdings auf, dass der Wortlaut mit "activities which […] may involve a violation of the criminal statutes" keine akute Rechtsverletzung fordert, sondern weit im Vorfeld einer Strafbarkeit ansetzt.[315] Eine hinreichende Tatsachengrundlage ist gerade nicht erforderlich. Die Schwelle ist vielmehr unter die für Beweiserhebungsmaßnahmen geltenden Standards abgesenkt.[316] Diese Absenkung wurde von den Gerichten akzeptiert. Eine Anhebung des *probable cause*-Standards auf diejenige des Title III wurde insofern als "inadequate to certain national security and intelligence needs" erachtet.[317]

Bei Personen, die weder die amerikanische Staatsbürgerschaft besitzen noch dauerhaft aufenthaltsberechtigt sind, den sogenannten *Non-U.S. Persons,* sind die Anforderungen zusätzlich abgesenkt.[318] Für die Einordnung als Agent einer ausländischen Macht genügt, wenn diese Person als Beamter einer ausländischen Re-

---

310 Vgl. *Keith*-Entscheidung 407 U.S. 297, 322 (1972); *Birkenstock,* Geo. L. J. (80) 1992, S. 863; *Kamisar/LaFave/Israel/King/Kerr,* S. 536. Die folgenden Ausführungen beziehen sich vor allem auf 50 U.S.C. § 1805 *(electronic surveillance)* und § 1824 *(physical searches)*.

311 Vgl. 50 U.S.C. § 1805(a)(3), 50 U.S.C. § 1824(a)(3) sowie E.O. 12333 von 2008 unter Punkt 2.5. Zudem muss das Zielobjekt die zu beobachtende Einrichtung nutzen.

312 50 U.S.C. § 1801(a).

313 50 U.S.C. §§ 1801(b)(2), 1821(1); vgl. *Grunwald,* S. 78; *Hall,* Wake Forest L. Rev. (41) 2006, S. 72.

314 Vgl. 50 U.S.C. § 1801(b)(2)(C) i.V.m. § 1801(c); 50 U.S.C. § 1801(b)(2)(D) i.V.m. 18 U.S.C. § 1001; 50 U.S.C. § 1801(b)(2)(E) i.V.m. 18 U.S.C. §§ 2, 371.

315 50 U.S.C. § 1801(b)(2)(A); vgl. *Birkenstock,* Geo. L. J. (80) 1992, S. 851f.

316 Vgl. *Standler*, S. 5.

317 Vgl. *United States v. Belfield,* 692 F.2d 141, 144 (D.C. Cir. 1982).

318 Zur Definition einer *U.S. Person* vgl. 50 U.S.C. § 1801(i).

gierung in den USA tätig wird, sich an Aktivitäten oder Vorbereitungshandlungen des internationalen Terrorismus, des Waffenhandels terroristischen Vereinigung beteiligt oder sich aus den Umständen eine Involvierung in geheimdienstliche Tätigkeiten ergibt.[319] Anders als bei der Beobachtung von *U.S. Persons* ist eine wissentliche Beteiligung nicht erforderlich. Diese Einstufung wird verschiedentlich kritisch gesehen.

In diesem Kontext wird vor allem die generelle Weite der vom FISA erfassten Beobachtungsobjekte kritisiert.[320] Die Nationalität und das entsprechende Anstellungsverhältnis seien nach § 1801(b)(1)(A) ein ausreichender Anknüpfungspunkt. Da der Nachweis eines Fehlverhaltens nicht erforderlich sei, wären vom Merkmal der ausländischen Macht i.S.d. 50 U.S.C. § 1801(a) auch überwiegend aus *Non-U.S. Persons* zusammengesetzte politische Organisationen erfasst. Ausgehend von dieser Definition könnten beispielsweise ausländische Staatsangehörige von Organisationen wie *Amnesty International* oder dem Internationalen Roten Kreuz taugliche Ziele einer FISA-Beobachtung sein.

Noch weiter geht das *lone wolf amendment* in 50 U.S.C. § 1801(b)(1)(C). Taugliches Beobachtungssubjekt sind danach sämtliche *Non-U.S. Persons*, die an Aktivitäten des internationalen Terrorismus vorbereitend oder sonstwie beteiligt sind. Im Anwendungsbereich dieser Vorschrift ist weder eine Verbindung zu einer ausländischen Macht oder Organisation noch der Verdacht strafbaren Handelns nachzuweisen.[321] Damit ergeben sich im Anwendungsbereich des FISA unterschiedliche Ermittlungsschwellen je nachdem, ob sich die Beobachtung gegen eine *U.S. Person* oder eine *Non-U.S. Person* richtet. Diese Unterscheidung kommt bereits im Gesetzeswortlaut zum Ausdruck. Während 50 U.S.C. § 1801(b)(2) auf "any person" Bezug nimmt, ist in § 1801(b)(1) von "any person other than a United States person" die Rede. Zwar können auch *U.S. Persons* im Bereich der Terrorismusbekämpfung nach 50 U.S.C. § 1801(a)(4) und in bestimmten Fällen von § 1801(a)(2), (3), (5), (6) tauglicher Gegenstand einer Überwachung i.S.d. 50 U.S.C. § 1801(2) sein,[322] allerdings werden durch das Erfordernis der Wissentlichkeit und der Verknüpfung zu einer ausländischen Macht höhere Anforderungen gestellt. Zudem darf die Einordnung als *agent of a foreign power* bei einer *U.S. Person* nicht ausschließlich auf der Wahrnehmung der Rechte aus dem ersten Zusatzartikel beruhen.[323]

Eine weitere Differenzierung erfolgt schließlich nach dem Einsatzort geheimdienstlicher Überwachungsmaßnahmen. Bei Beobachtungsmaßnahmen im Ausland

---

319 Vgl. 50 U.S.C. § 1801(b)(1)(A)–(B).

320 Vgl. zur nachfolgenden Kritik *Cole* 2005; *Kris/Wilson,* § 11:19, S. 436.

321 Vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 72; *Liu,* CRS 2011, S. 1.

322 So *Standler*, S. 5.

323 50 U.S.C. § 1805(a)(2)(A).

sinken die Erhebungsschwellen erneut, da diese zum Teil von den Vorgaben des vierten Verfassungszusatzes entbunden sind.[324] Ausländer im Ausland sind überwiegend vom Schutz des vierten Verfassungszusatzes ausgenommen.[325] Selbst in Bezug auf US-Bürger sind die Schutzstandards abgesenkt, da das Vertrauen in den Schutz der Privatsphäre bei einem Auslandsaufenthalt niedriger anzusetzen ist als bei einem Aufenthalt im Inland.[326] Nach den einschlägigen Regelungen genügt für die Auslandsüberwachung neben der Verbindung zu einer ausländischen Macht der vernünftige Glaube daran, dass sich die zu beobachtende Person an ihrem Aufenthaltsort befindet, um dort zu spionieren.[327] Auf das *probable cause*- und das *warrant*-Erfordernis wird demnach vollständig verzichtet.[328]

In der Gesamtbetrachtung sind die Ermittlungsschwellen des FISA gegenüber sonstigen staatlichen Ermittlungen vergleichsweise stark abgesenkt beziehungsweise modifiziert. Charakteristisch ist die Unterscheidung zwischen Beobachtungsmaßnahmen im In- und Ausland sowie der Überwachung von *U.S. Persons* und *Non-U.S. Persons*.[329]

bb) Ende geheimdienstlicher Ermittlungen

Die Dauer geheimdienstlicher Ermittlungen wird nicht durch bestimmte Verdachtsschwellen begrenzt. Dies gilt aufgrund der Geltung des Opportunitätsprinzips in gleicher Weise für Ermittlungen zu Polizei- und Strafverfolgungszwecken, sodass sich diesbezüglich keine Abweichungen ergeben.[330]

cc) Zwischenergebnis zu zeitlichen Rahmenbedingungen

Im amerikanischen Recht sind Ermittlungsmaßnahmen außerhalb des vierten Verfassungszusatzes an keine zeitlichen Rahmenbedingungen gebunden.[331] Dies gilt sowohl für polizeiliche, strafprozessuale als auch geheimdienstliche Ermittlun-

---

[324] Vgl. *Markwordt Skehan,* S. 117.

[325] Vgl. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (S. Ct. 1990) sowie *Litt/Bennett,* in: Wittes, S. 154.

[326] Eine inhaltliche Begrenzung erfolgt durch E.O. 12333 von 2008, der unter Punkt 2.4 und 2.5 eine Genehmigung des *Attorney General* und eine Subsidiaritätsklausel vorsieht.

[327] Vgl. 50 U.S.C. § 1881b(c)(1)(B) bzw. 50 U.S.C. § 1881a(a). Darin heißt es: "reasonably believed to be located outside the United States to acquire foreign intelligence information".

[328] Vgl. *Kris,* in: Wittes, S. 229. Diese Besonderheit besteht erst seit der FISA-Reform im Jahre 2008.

[329] Vgl. *Smith/Howe,* in: Markle Foundation, S. 134f.

[330] Vgl. zur Bindung an das Opportunitätsprinzip *Perron,* in: ders., S. 499; *Reinbacher,* S. 30, 171.

[331] Vgl. *Arzt,* Überwachungsmaßnahmen, S. 22.

gen. Ist der Anwendungsbereich der *search and seizure*-Maßnahmen eröffnet, orientieren sich geheimdienstliche Ermittlungen je nach Aufklärungsrichtung an abweichenden Ermittlungsschwellen und Zielobjekten. Während rein inländische Ermittlungen offiziell weiterhin den Vorgaben des vierten Verfassungszusatzes unterliegen, sind die Anforderungen an Ermittlungen mit Auslandsbezug stark abgesenkt. Im Anwendungsbereich des FISA sind die Voraussetzungen für Maßnahmen im Ausland sowie bei Überwachungen von *Non-U.S. Persons* sogar noch niedriger. Diese Unterschiede verlieren jedoch seit der Ersetzung durch den *significant purpose*-Standard und dem Verschwinden der *wall* an Bedeutung.[332] Die parallele Verfolgung strafrechtlicher Belange stellt kein Hindernis mehr dar.[333]

d) Durchsetzungsmöglichkeiten

Bei einer Untersuchung der Durchsetzungsmöglichkeiten sind vor allem die gegenüber der CIA bestehenden Einschränkungen auffallend. Diese soll nach der ausdrücklichen Formulierung des Gesetzes weder über Strafverfolgungs- und Zwangsbefugnisse verfügen noch Sicherheitsfunktionen im Inneren wahrnehmen.[334] Dieser Vorbehalt wurde mit der Gründung der CIA durch den *National Security Act* von 1947 festgeschrieben. Offizielle Begründung für diese Regelung war das nach dem Zweiten Weltkrieg bestehende Misstrauen gegenüber gestapoähnlichen Strukturen.[335] Tatsächlich spielte jedoch die zum damaligen Zeitpunkt bestehende Vormachtstellung des FBI eine erhebliche Rolle. Dieses wollte seine Vorrechte im Inneren wahren und einen möglichen Kompetenzverlust zugunsten der CIA verhindern.[336] Die Bedeutung dieses zweiten Aspekts zeigt sich bereits darin, dass auf die Übertragung vergleichbarer Beschränkungen auf die anderen amerikanischen Geheimdienste verzichtet wurde. Gerade das FBI vereinigt polizeiliche und geheimdienstliche Befugnisse in einer Behörde.[337] Dementsprechend können aus dem Vorbehalt gegenüber der CIA keine allgemeinen Schlussfolgerungen zum amerikanischen Geheimdienstwesen insgesamt gefolgert werden. Dies gilt umso mehr, als die tatsächliche limitierende Wirkung aufgrund der sehr vagen

---

332 Vgl. *M. McCarthy,* Harv. J. Leg. (39) 2002, S. 444.

333 Kritisch *Arzt,* in: Graulich/Simon, S. 261; *Grunwald,* S. 122.

334 In 50 U.S.C. § 403-4a(d)(1) heißt es: "shall have no police, subpoena, or law enforcement powers or internal security functions"; vgl. zudem E.O. 12333 von 2008 unter Punkt 2.4.(a) sowie *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 416.

335 Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 335; *Hitz,* Harv. J. L. & Pub. Pol'y (25) 2002, S. 769; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 416; *Treverton,* Intelligence, S. 1.

336 Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 335; *Hitz,* Harv. J. L. & Pub. Pol'y (25) 2002, S. 769; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 416.

337 Vgl. hierzu *Grunwald,* S. 121.

Formulierung des Vorbehalts zweifelhaft ist.[338] Lediglich die elektronische Überwachung im Inland wird ausdrücklich als solche in der E.O. 12333 von 2008 unter Punkt 2.4(a) ausgeschlossen. In den übrigen Fällen ist weitgehend unklar, welche Befugnisse die CIA gegen wen und wo einsetzen darf.[339]

Bei einer Betrachtung der übrigen Geheimdienste wird ebenfalls deutlich, dass deren Kompetenzen in aller Regel nicht auf die Informationssammlung beschränkt sind, sondern auch aktive Maßnahmen umfassen. Mittels der sogenannten *subpoena*-Befugnisse können sie unter anderem verwaltungsrechtliche Verfügungen erlassen und damit Behörden, Unternehmen und sogar Privatpersonen zur Herausgabe der bei ihnen vorhandenen Daten, Unterlagen und Gegenstände verpflichten.[340] Eine besondere Form dieser Verfügung stellen die bereits beschriebenen *National Security Letter* dar, durch welche der Betroffene zur Herausgabe von Finanz-, Telefon- und Emaildaten verpflichtet werden kann.[341] Bestimmte Zwangsbefugnisse werden den Geheimdiensten nur im Ausnahmefall vorenthalten. Ein Beispiel dafür ist etwa der Rückgriff auf *grand jury investigations,* durch welche die Staatsanwaltschaft das Erscheinen des Zeugen forcieren kann.[342] Eine vergleichbare Anwesenheitspflicht kann weder durch die National Security Letters noch aufgrund anderer Maßnahmen nach dem FISA erzwungen werden.[343] Von derartigen Ausnahmekonstellationen abgesehen sind die amerikanischen Geheimdienste grundsätzlich berechtigt, selbst Konsequenzen aus den erzielten Erkenntnissen zu ziehen und aktive Gefahrenabwehrmaßnahmen zu ergreifen.

e) Ausgewählter Vergleich der Erhebungsvoraussetzungen

Nachfolgend werden die allgemeinen Besonderheiten der geheimdienstlichen Erhebungsvoraussetzungen herausgearbeitet.

aa) Allgemeine Anforderungen

Die im Vergleich zur Beweiserhebung festzustellenden Unterschiede nehmen mit steigender Eingriffsintensität der Ermittlungsmethode zu. Allgemein wird zwischen Maßnahmen der *threat assessment* einerseits und Maßnahmen der *preliminary* und

---

338 Vgl. *Harris,* Yale L. & Pol'y Rev. (23) 2005, S. 533; *Hörauf,* S. 291; *Ortiz,* in: Markle Foundation, S. 95.

339 So *Harris,* Yale L. & Pol'y Rev. (23) 2005, S. 533.

340 50 U.S.C. § 1861(a)(1), der mit der Herausgabe von "any tangible things" sämtliche beweglichen Gegenstände, u.a. Bücher, Aufnahmen, Dokumente erfasst; vgl. allgemein *Arzt,* in: Graulich/Simon, S. 262; *Grunwald,* S. 182.

341 Vertiefend *Arzt,* in: Graulich/Simon, S. 262; *Doyle,* CRS 2011; *Grunwald,* S. 213.

342 Vgl. hierzu *United States v. Enterprises*, Inc., 498 U.S. 292, 298 (S. Ct. 1991); *Kris/Wilson,* § 11:18, S. 435.

343 Vgl. *Kris/Wilson,* § 11:18, S. 435.

full investigations nach dem Title III und dem FISA andererseits differenziert. An Maßnahmen der *threat assessment* werden inhaltlich keine bedeutsamen Anforderungen gestellt.[344] Erforderlich und ausreichend ist die Verfolgung eines geheimdienstrelevanten Erhebungszwecks. Danach muss die Informationserhebung der Aufdeckung beziehungsweise Verhinderung von Bundesstraftaten oder Bedrohungen der nationalen Sicherheit dienen oder für Zwecke der Auslandsaufklärung notwendig sein.[345] Da bei Maßnahmen der Gefahreinschätzung die erforderliche Geheimdienstrelevanz unter anderem bei einer Begehung von Bundesstraftaten bejaht wird, können diese durch den Strafverfolgungs- und Geheimdienstsektor unter identischen Voraussetzungen genutzt werden. Im Bereich der *preliminary* und *full investigations* richten sich die konkreten Anforderungen nach der jeweiligen Aufklärungsrichtung der Maßnahme. Lediglich die Überwachung auslandsbezogener Sachverhalte (FII) hat im FISA eine Sonderregelung erfahren, während die Überwachung eines rein inländischen Sachverhalts (DII) im Anwendungsbereich des vierten Verfassungszusatzes weitgehend an die Vorgaben der strafrechtlichen Ermächtigungsgrundlagen gebunden ist. Die unterschiedlichen Erhebungsvoraussetzungen beruhen dementsprechend auf abweichenden verfassungsrechtlichen Schutzstandards, die für rein inlands- oder auslandsbezogene Sachverhalte gelten. Die Differenzierung zwischen Polizeirecht einerseits und Geheimdienstrecht andererseits spielt demgegenüber eine untergeordnete Rolle.

bb) Einsatz Verdeckter Ermittler

Anknüpfend an die vorangegangenen Ausführungen unterliegen polizeiliche und geheimdienstliche Ermittlungen bei rein inlandsbezogenen Sachverhalten oftmals identischen Erhebungsvoraussetzungen, während für die Überwachung auslandsbezogener Sachverhalte Sonderregeln im FISA existieren. Eine der wenigen Ausnahmen bildet der Einsatz sogenannter *undercover agents*.[346] Deren Einsatz steht bei der Verfolgung geheimdienstlicher Zwecke insgesamt im Ermessen der Ermittlungsbeamten, das heißt sowohl bei Maßnahmen der DII als auch der FII. Da das Vertrauen in die wahre Identität einer Person nicht durch den vierten Verfassungszusatz geschützt wird, besteht keine Notwendigkeit Maßnahmen der DII an die strafrechtlichen Ermächtigungsgrundlagen zu binden.[347] Eine formale Zustimmung ist nur dann erforderlich, wenn von den Ermittlungen religiöse oder politische Organisationen betroffen sind.[348]

---

[344] Einzelne Fragestellungen richten sich nach dem *FBI Domestic Investigations and Operations Guide* (DIOG), der mehr als 600 Seiten umfasst. Zu finden unter www.fbi.gov.

[345] Mukasey Guidelines 2008, II.A.1.

[346] Vgl. Mukasey Guidelines 2008, V.A.7; *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 166.

[347] Vgl. *Trüg,* S. 411f; *Signorelli,* S. 233ff.

[348] In diesem Fall ist auch die *National Security Division* zu beteiligen.

Die Anforderungen an den Einsatz eines *undercover agent* bei rein strafrechtlichen Ermittlungen sind im Vergleich dazu erhöht. Dieser ist zusätzlich an die umfassenden Anforderungen der Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations von 2002 gebunden.[349] Diese fordern unter anderem die schriftliche Anordnung durch einen *special agent in charge* (SAC), die Bewilligung des *FBI Headquarters*, Angaben zur Notwendigkeit der Maßnahme sowie eine strikte Kosten-Nutzen-Analyse unter Beachtung des Subsidiaritätsprinzips.[350] Von derartigen Besonderheiten abgesehen sind die Erhebung von *domestic intelligence* und die Erhebung von Beweismaterial an identische verfassungsrechtliche Bedingungen gebunden.

cc) Elektronische Überwachungsmaßnahmen

Im Bereich der elektronischen Überwachungsmaßnahmen bestehen zwischen Maßnahmen der DII und der FII deutliche Unterschiede. Die Anforderungen unterscheiden sich danach, ob es sich um einen auslandsbezogenen oder einen rein inländischen Sachverhalt handelt. Elektronische Überwachungsmaßnahmen zu Zwecken der DII unterliegen den strafrechtlichen Vorgaben der 18 U.S.C. §§ 2510ff (Title III). Da die einschlägigen Mukasey Guidelines 2008 keine Unterscheidung zwischen geheimdienstlichen und polizeilichen Ermittlungen vornehmen, sind bei rein inländischen Sachverhalten beide Ermittlungszweige überwiegend an identische Voraussetzungen gebunden.

Die Überwachung auslandsbezogener Sachverhalte unterliegt demgegenüber dem FISA, der erheblich von den Anforderungen des Title III abweicht.[351] Die unterschiedlichen Voraussetzungen beider Regelwerke werden im Folgenden in Bezug auf die tauglichen Zielobjekte und Örtlichkeiten sowie die Anforderungen an die Bestimmtheit, die Verhältnismäßigkeit und etwaigen Speicherpflichten verdeutlicht.

(1) Taugliche Zielobjekte

Die genannten Regelwerke knüpfen die elektronische Überwachung an unterschiedliche Zielobjekte. Im Anwendungsbereich des FISA nach 50 U.S.C. §§ 1801–1812 muss sich die Überwachung gegen eine ausländische Macht oder

---

[349] Deren Anwendungsbereich ist nach Punkt III der Richtlinie auf "general crimes investigations, and criminal intelligence investigations" begrenzt und kann damit als Gegenstück zu geheimdienstlichen Ermittlungen herangezogen werden.

[350] Vgl. hierzu Punkt IV.A sowie IV.B. (1), (2) der Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations von 2002.

[351] Vertiefend zu den Voraussetzungen *Gurulé/Corn,* S. 218ff, 232ff.

einen ihrer Agenten richten.[352] Das Merkmal „ausländische Macht" erfasst ausländische Regierungen, politische Organisationen sowie Gruppierungen des internationalen Terrorismus.[353] Bei der Einstufung als Agent einer ausländischen Macht wird zwischen *U.S. Persons* und *Non-U.S. Persons* differenziert. Die Beobachtung einer *U.S. Person* setzt in der Regel die wissentliche Beteiligung an Spionage- und Sabotagetätigkeiten beziehungsweise Akten des internationalen Terrorismus voraus, während bei *Non-U.S. Persons* auf dieses Wissenselement verzichtet wird.[354] Für die Einordnung des Zielobjekts dürfen vergangene Aktivitäten berücksichtigt werden, sodass für eine Überwachung kein aktueller Verdacht erforderlich ist.[355]

Wesentlicher Zweck der Informationserhebung ist der Erhalt von *foreign intelligence information*.[356] Die Informationserhebung ist damit nicht primär auf den Erhalt von Beweismaterial gerichtet, sondern betrifft Erkenntnisse, die eine Bedrohung der nationalen Sicherheit durch eine ausländische Macht zum Gegenstand haben. Diese Zielsetzung ist durch einen hochrangigen Beamten zu bescheinigen.[357] Sofern der vorgenannte Nachweis eines tauglichen Zielobjekts erbracht wurde, wird von diesem regelmäßig auf die Rechtmäßigkeit des Überwachungsziels geschlossen.[358]

Die vergleichsweise heranzuziehende strafprozessuale Telekommunikationsüberwachung nach 18 U.S.C. §§ 2510ff (Title III) weicht von diesen Voraussetzungen erheblich ab. Während der FISA den Verdacht eines bestimmten Zielobjekts genügen lässt, muss sich der *probable cause* im Rahmen des Title III auf eine der in 18 U.S.C. § 2516 genannten Katalogstraftaten beziehen.[359] Im Gegensatz dazu ist im FISA weder die Identifizierung eines Verdächtigen noch der Nachweis illegalen Verhaltens erforderlich.[360] Die Bezugspunkte des FISA und des Title III sind damit sehr unterschiedlich.

---

352 50 U.S.C. § 1804(a)(3)(A); vgl. auch *Hall,* Wake Forest L. Rev. (41) 2006, S. 71; *Smith/Howe,* in: Markle Foundation, S. 140.

353 50 U.S.C. § 1801(a).

354 Vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 72.

355 50 U.S.C. § 1805(b) bzw. 1824(b); vgl. *Kris/Wilson,* § 11:5, S. 399.

356 Siehe 50 U.S.C. § 1804(a)(6); vgl. *Kris/Wilson,* § 11:6, S. 406. Zum Verzicht auf den *primary purpose* vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 151.

357 50 U.S.C. §§ 1804(a)(6)(A); *Hall,* Wake Forest L. Rev. (41) 2006, S. 73f.

358 So *Grunwald,* S. 102.

359 Vgl. 18 U.S.C. § 2518(3)(a) i.V.m. § 2516; vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 81; *Liu,* CRS 2011, S. 3. *Smith/Howe,* in: Markle Foundation, S. 138; *Trüg,* S. 408. Diese Hürde wurde durch die Aufnahme einer Vielzahl an Delikten erheblich abgesenkt.

360 Vertiefend *Kris/Wilson,* § 6:14.

(2) Tauglicher Bezugspunkt der Überwachung

Als zweite Voraussetzung muss für eine FISA-Überwachung zwischen dem Zielobjekt und der zu überwachenden Örtlichkeit eine gewisse Verknüpfung bestehen.[361] Der erforderliche Nexus ist zu bejahen, wenn die Räumlichkeit durch die ausländische Macht genutzt wurde beziehungsweise aktuell oder künftig genutzt wird.[362] Die Räumlichkeit selbst muss in keiner Verbindung zur Einstufung des Ziels als ausländische Macht stehen. Ein konkreter Nachweis, wonach die Abhörmaßnahmen tatsächlich konkrete Bedrohungslagen aufdecken werden, ist nicht erforderlich.[363]

Im Vergleich dazu muss im Anwendungsbereich des Title III ein hinreichender Grund dafür vorliegen, dass während der aufgezeichneten Kommunikation Informationen über die besagte Straftat anfallen.[364] Darüber hinaus ist nach Title III ein Konnex zwischen der fraglichen Straftat und der überwachten Kommunikation sowie der überwachten Örtlichkeit erforderlich.[365] Die vergleichende Betrachtung des Title III und des FISA deckt damit erneut erhebliche Unterschiede auf.

(3) Bestimmtheit der Anordnung

Darüber hinaus werden im FISA und Title III unterschiedliche Anforderungen an die Bestimmtheit der Überwachungsanordnung gestellt.[366] Der für strafrechtliche Ermittlungen geltende vierte Verfassungszusatz fordert eine hinreichend klare Festlegung von Ziel, Methode und Dauer der Überwachungsmaßnahme.[367] Bei einer Telekommunikationsüberwachung nach Title III werden diese Angaben in 18 U.S.C. § 2518(4)(a)–(d) präzisiert. Nach 18 U.S.C. § 2518(4)(c) ist unter anderem eine "particular description" von Beschaffenheit und Lage der überwachten Einrichtung sowie eine spezifische Beschreibung der abzuhörenden Kommunikation und der darauf bezogenen Straftat erforderlich.

Im Unterschied dazu wird bei einer FISA-Anordnung nach 50 U.S.C. § 1805(c)(1)(A)–(E) auf eine genaue Beschreibung der zu überwachenden Kommunikation verzichtet. Es genügen vielmehr generelle Angaben zur Art der Kom-

---

361 Vgl. *Kris/Wilson,* § 6:14; § 11:6, S. 407.

362 50 U.S.C. § 1804(a)(3)(B); vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 83.

363 Vgl. *Grunwald,* S. 107.

364 18 U.S.C. § 2518(3)(b); vgl *Grunwald,* S. 105; *Hall,* Wake Forest L. Rev. (41) 2006, S. 81.

365 18 U.S.C. § 2518(3)(d). Der Konnex zur Örtlichkeit kann aufgrund der erfolgten oder beabsichtigten Tatbegehung in der überwachten Räumlichkeit oder der sonstigen Nutzung durch den Täter vorliegen; vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 82.

366 Vgl. *Grunwald,* S. 108.

367 Vgl. *Berger v. New York*, 388 U.S. 41, 84ff (1967); *Vervaele,* Utrecht L. Rev. (1) 2005, S. 5.

munikation.[368] Die überwachte Örtlichkeit ist nur bei vorhandener Kenntnis zu benennen.[369] Die an eine FISA-Anordnung zu stellenden Bestimmtheitsanforderungen bleiben damit hinter den Voraussetzungen des Title III zurück.

(4) Verhältnismäßigkeitsgesichtspunkte

Weitere Unterschiede ergeben sich in Bezug auf die sogenannten *minimization procedures*. Hierbei handelt es sich um eine Art formalisierte Verhältnismäßigkeitskontrolle, welche die Sammlung, Speicherung und Weitergabe von Daten zum Schutz der Privatsphäre auf das erforderliche Minimum begrenzt.[370] Diese Verfahrensregeln reduzieren im Anwendungsbereich des Title III den Umfang der Informationserhebung, da Vorgänge ohne Relevanz für die Ermittlungen beispielsweise erst gar nicht aufgezeichnet werden dürfen.[371] Lediglich für Gespräche in verschlüsselter oder ausländischer Sprache wird diese Vorgabe kurzfristig aufgehoben und die Aussortierung auf eine nachträgliche Kontrolle verschoben. Diese muss allerdings unverzüglich nach Abschluss der Überwachung erfolgen.[372] Für die FISA-Überwachung fehlen solche strikten beziehungsweise zeitlichen Bindungen.[373] Dort dürfen zunächst alle nicht offensichtlich irrelevanten Informationen erhoben werden.[374]

(5) Einhaltung der Speicherungspflichten

Die Unterschiede setzen sich in Bezug auf das sogenannte *sealing requirement* fort. Bei strafrechtlichen Überwachungsmaßnahmen führt diese Vorgabe dazu, dass alle Erkenntnisse aus rechtmäßig aufgezeichneten strafrechtlichen Überwachungs-

---

[368] 50 U.S.C. § 1805(c)(1)(C) spricht von "the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance".

[369] Anders als Title III enthält 50 U.S.C. § 1805(c)(1)(B) den Zusatz "if known".

[370] Vgl. etwa 50 U.S.C. § 1801(h)(1). Dieser beschreibt die *minimization procedures* unter anderem als "specific procedures […] that are reasonably designed […] to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information"; vgl. *Grunwald,* S. 82. Vertiefend zu *minimization procedures* des FISA vgl. *Kris/Wilson,* § 9.

[371] Vgl. *Kris/Wilson,* § 9:5, S. 338.

[372] 18 U.S.C.§ 2518(5): "minimization may be accomplished as soon as practicable"; vgl. auch *Kris/Wilson,* § 11:10, S. 414.

[373] Siehe hierzu die *minimization procedures* in 50 U.S.C. § 1801(h)(1) (elektronische Überwachungsmaßnahmen), § 50 U.S.C. § 1821(4) (Durchsuchungen) und in 50 U.S.C. § 1861(g) (Herausgabe von Dokumenten). Diese sind auf *U.S. Persons* begrenzt; vgl. vertiefend *Kris/Wilson,* § 11:10.

[374] Vgl. *Kris/Wilson,* § 9:5, S. 335.

maßnahmen nach Ablauf der Anordnung gespeichert und versiegelt werden.[375] Dieses Erfordernis soll die Integrität des eventuell darin enthaltenen Beweismaterials gewährleisten.[376] Die Existenz dieses Siegels bildet eine Grundvoraussetzung für die spätere Verwertung als Beweismittel, sodass dessen Fehlen einer hinreichenden Begründung bedarf.[377]

Im FISA fehlt eine vergleichbare Verpflichtung. Lediglich die FISA-Anordnungen selbst müssen für zehn Jahre gespeichert werden, nicht jedoch die aufgezeichneten Inhalte.[378] Der Gesetzgeber ging davon aus, dass der Schutz der Privatsphäre im FISA durch eine nachträgliche Durchsicht und Vernichtung irrelevanter Erkenntnisse gewährleistet werden könnte. Die umfassende FISA-Erhebung soll daher theoretisch durch eine limitierte Speicherung und Weitergabe kompensiert werden.[379] Dementsprechend sind nach dem FISA nur geheimdienstlich relevante Erkenntnisse systematisch zu erfassen, während die übrigen Informationen zu löschen sind.[380] Die geforderte Zerstörung irrelevanter Informationen wird in der Praxis allerdings nicht immer umgesetzt.[381]

(6) Zwischenergebnis

Die elektronische Überwachung nach dem FISA weicht damit in mehreren Aspekten von den Voraussetzungen des Title III ab. Während nach Title III Telekommunikationsdaten nur begrenzt erhoben werden dürfen, ist nach dem FISA eine umfassende Erhebung gestattet. Umgekehrt sind nach Title III die tatsächlich erhobenen Erkenntnisse vollumfänglich zu speichern und dokumentieren, während im FISA eine vergleichbare Pflicht fehlt.[382] Diese Erkenntnisse sind weitgehend auf die sonstigen Erhebungsmethoden des FISA übertragbar.[383]

---

375 Vgl. 18 U.S.C. § 2518(8)(a): "Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions."

376 Vgl. *Kris/Wilson,* § 11:10. *United States v. Ojeda Rios*, 495 U.S. 257 (S. Ct. 1990): "the sealing requirement is important precisely because it limits the Government's opportunity to alter the recordings".

377 Vgl. 18 U.S.C. § 2518(8)(a): "The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517."

378 Vgl. 50 U.S.C. § 1805(g), § 1824(f), sowie *Kris/Wilson,* § 11:10.

379 Vgl. *Kris/Wilson,* § 11:10.

380 Vgl. *Kris/Wilson,* § 9:5, S. 336.

381 Vgl. *Kris/Wilson,* § 9:5, S. 336.

382 Vgl. insgesamt *Kris/Wilson,* § 9:4; § 9:5, S. 338; § 11:10, S. 413f.

383 Siehe zum Vergleich von Durchsuchungsmaßnahmen *Hall,* Wake Forest L. Rev. (41) 2006, S. 85ff.

dd) Zwischenergebnis

Durch den Vergleich vereinzelter Ermittlungsmethoden wurde deutlich, dass die konkreten Erhebungsvoraussetzungen maßgeblich durch die Einteilung in *domestic intelligence investigations* und *foreign intelligence investigations* bestimmt werden. Da im Bereich der DII keine den Verfassungsvorgaben entsprechende Spezialermächtigung geschaffen wurde, unterliegen diese im verfassungsrelevanten Bereich den Anforderungen der strafrechtlichen Ermächtigungsgrundlagen, wie etwa dem dargestellten Title III. Geheimdienstliche Ermittlungen mit Auslandsbezug sind demgegenüber an die Vorgaben des FISA gebunden.[384] Dieser stellt in den meisten Fällen geringere Anforderungen und ermöglicht zugleich eine umfassendere Informationserhebung. Insbesondere im Rahmen der Telekommunikationsüberwachung konnte verdeutlicht werden, dass Ermittlungsbeamte auf der Grundlage des FISA viel früher und umfassender Gespräche aufzeichnen können als auf der Grundlage des Title III. Die Tatsache, dass der FISA mit der Einführung des *significant purpose*-Standards im Jahr 2001 zumindest teilweise zu Strafverfolgungszwecken eingesetzt werden darf, hat sich folglich nicht in den einzelnen Erhebungsvoraussetzungen niedergeschlagen.

f) Kontrollmechanismen und Verfahrensablauf

Der großen Zahl amerikanischer Geheimdienste stehen ebenso zahlreiche Kontrollmechanismen gegenüber.[385] Die Darstellung konzentriert sich daher auf die vorliegend zentralen Kontrollinstanzen und -vorgänge.

aa) Relevante Kontrollinstanzen

Die zur Kontrolle der Geheimdienste berufenen Instanzen lassen sich überwiegend den drei Staatsgewalten zuordnen.

(1) Kontrolle durch die Exekutive

Im Bereich der Exekutivkontrolle werden die Kontrollaufgaben vor allem durch den *Director of National Intelligence* (DNI) und den *National Security Council* (NSC) wahrgenommen. Daneben sind das *President's Intelligence Advisory Board* (PIAB) und das ihm angehörende *Intelligence Oversight Board* (IOB) von Bedeutung. Der DNI ist Leiter und Koordinator des Gemeindienstsektors sowie Berater

---

384 Daneben existieren weitere Ermächtigungen, deren Darstellung allerdings den Rahmen dieses Überblicks sprengen würde.

385 Vgl. *Hörauf,* S. 293, der von etwas weniger als 20 Einrichtungen spricht.

des Präsidenten, des NSC und des *Homeland Security Councils* in nationalen Sicherheitsfragen.[386] Er untersteht direkt dem Präsidenten, der ihn ernennt und kontrolliert.[387] Neben Koordinierungsaufgaben obliegt dem DNI die Aufsicht über den Geheimdienstsektor. Er soll unter anderem die Einhaltung gesetzlicher und verfassungsrechtlicher Vorgaben und eine effektive Aufgabenwahrnehmung sicherstellen.[388] Zudem ist er zur Durchführung des *National Intelligence Programs* mit verschiedenen Budgetrechten ausgestattet.[389]

In seiner Arbeit wird der DNI durch verschiedene Berater unterstützt. Zu diesen zählt unter anderem der *Civil Liberties Protection Officer* (CLPO). Dieser stellt sicher, dass der gesetzlich und verfassungsrechtlich vorgegebene Schutz der Privatsphäre und der Bürgerrechte durch die Dienste eingehalten wird.[390] Entsprechenden Beschwerden kann er nachgehen. Daneben kann der DNI auf den *National Intelligence Council* zurückgreifen. Dieses vom *National Security Council* zu unterscheidende Expertengremium wird durch den DNI besetzt. Es analysiert und bewertet behördenübergreifend die Produktion von Geheimdienstinformationen und dient der mittel- und langfristigen Strategieentwicklung.[391] Der bereits erwähnte *National Security Council* (NSC) ist ein weiterer Aufsichtsakteur, der als ranghöchste Einheit den Präsidenten in sicherheitspolitischen Fragestellungen berät.[392] Ihm gehören neben dem Präsidenten unter anderem der Vizepräsident, der Außen-, Verteidigungs- und Wirtschaftsminister an.[393] Der NSC überprüft in regelmäßigen Zeitabständen die Rechtmäßigkeit, Effektivität und politische Konformität durchgeführter und laufender eingriffsintensiver Geheimdienstmaßnahmen.[394] Der Fokus liegt auf der politischen Kontrolle.[395] Das ebenfalls genannte *President's Intelligence Advisory Board* (PIAB) besteht aus 16 vom Präsidenten zu benennenden Nichtregierungsmitgliedern. Es wird ebenfalls beratend für den Präsidenten tätig und informiert diesen über die Effektivität und Qualität der geheimdienstlichen

---

386 50 U.S.C. § 403(b); E.O. 12333 von 2008 unter Punkt 1.3; vgl. zudem *Hörauf,* S. 313. Diese Aufgaben wurden früher vom DCI, dem Director der CIA, wahrgenommen.

387 50 U.S.C. § 403(a)(1), (b).

388 50 U.S.C. § 403–1(f)(2), (4). Namentlich genannt werden vor allem die CIA und das *National Counterterrorism Center*.

389 Vgl. hierzu den offiziellen Internetauftritt unter http://www.dni.gov/faq_about.htm [Stand: 1.5.2012].

390 Vgl. zu dessen Befugnissen 50 U.S.C. § 403–3d. Daneben existiert das durch den Präsidenten besetzte *Privacy and Civil Liberties Oversight Board* (PCLOB), das den Kongress jährlich über die Berücksichtigung von Bürgerrechten im Kampf gegen den Terrorismus informiert, vgl. 42 U.S.C. § 2000ee; *Hörauf,* S. 325f.

391 50 U.S.C. § 403–3b; vgl. auch *Hörauf,* S. 294, 325.

392 50 U.S.C. § 402 (a), vgl. ebenfalls E.O. 12333 von 2008 unter Punkt 1.2(a) und (b), sowie http://www.whitehouse.gov/administration/eop/nsc/. [Stand: 1.5.2012].

393 50 U.S.C. § 402 (a).

394 E.O. 12333 von 2008 unter Punkt 1.2(b); *Hörauf,* S. 330f.

395 Vgl. stellvertretend *Hörauf,* S. 295.

Aufgabenwahrnehmung. Zu diesem Zweck überprüft das dem PIAB zugeordnete, meist vierköpfige *Intelligence Oversight Board* (IOB) Einzelmaßnahmen der Geheimdienste auf die Einhaltung verfassungsrechtlicher, gesetzlicher und präsidialer Vorgaben.[396] Die Dienste müssen mit diesen Einrichtungen kooperieren und dem PIAB vierteljährlich über die durchgeführten Maßnahmen beziehungsweise dem IOB über mögliche gesetzeswidrige Geheimdienstaktivitäten berichten.[397] Die Erkenntnisse werden aufbereitet und dem Präsidenten in halbjährlichen Berichten zur Verfügung gestellt.

(2) Kontrolle durch die Judikative

Die gerichtliche Kontrolle unterteilt sich bei geheimdienstlichen Angelegenheiten in die klassische Bundesgerichtsbarkeit einerseits und die Sondergerichtsbarkeit des *Foreign Intelligence Surveillance Court* (FISC) andererseits. Die Bundesgerichtsbarkeit ist im Anwendungsbereich des vierten Verfassungszusatzes vor allem für die Kontrolle rein inlandsbezogener Erhebungsmaßnahmen (DII) zuständig. Sie greift zudem bei Bekanntwerden gravierender Missbrauchsfälle beziehungsweise bei Verstößen gegen nationales und internationales Recht.[398]

Der FISC kontrolliert wiederum Maßnahmen auf der Grundlage des FISA. Er wurde 1978 geschaffen und bildet einen Gerichtszweig außerhalb der verfassungsrechtlich vorgegebenen Bundesgerichtsbarkeit. Die Vorgaben zur Konzeption dieses Gerichts finden sich daher nicht in 28 U.S.C. §§ 1–482 *(Judiciary),* sondern in 50 U.S.C. § 1803 *(War and National Defense)*. Die FISC-Richter entstammen der zivilen Bundesgerichtsbarkeit, die vom Gerichtspräsidenten des *Supreme Court* ernannt werden.[399] Zum Schutz nationaler Sicherheitsinteressen erfolgen sämtliche Verfahrensvorgänge in einem geheimen, nicht kontradiktorischen Verfahren.[400] Die exakte Geheimhaltungsstufe wird durch den Gerichtspräsidenten, den *Attorney General* und den DNI festgelegt.[401] Entscheidungen des FISC können in der Berufungsinstanz vor dem FISCR *(Foreign Intelligence Surveillance Court of Review)* und diese vor dem *Supreme Court* angegriffen werden.[402] Die Einrichtung dieser Sonderzuständigkeit wird mit den besonderen Bedürfnissen der auslands-

---

396 Vgl. hierzu den offiziellen Internetauftritt unter www.whitehouse.gov/administration/eop/piab [Stand: 1.5.2012].

397 E.O. 12333 von 2008 unter Punkt 1.6(c); *Hörauf,* S. 331.

398 So *Lundberg,* in: Baldino, S. 62f. Bei politischen Sachverhalten kommt es zusätzlich zur Errichtung von Sonderkommissionen wie dem *Church Committee*, die eine unabhängige Aufklärung gewährleisten sollen, vgl. *Hörauf,* S. 304.

399 Vgl. *Arzt,* in: Graulich/Simon, S. 258; *McNamara,* in: Markle Foundation, S. 90.

400 Sog. Verfahren *under seal* bzw. *under security measures*. 50 U.S.C. § 1803(a), (b), (c), vgl. *Standler*, S. 6f; *Smith/Howe,* in: Markle Foundation, S. 140.

401 50 U.S.C. § 1803(c).

402 50 U.S.C. § 1803.

bezogenen, nachrichtendienstlichen Aufklärung begründet, denen die zeitintensive und aufwändige klassische richterliche Anordnung nach Ansicht des Gesetzgebers nicht ausreichend Rechnung trägt.[403] Der FISC könne nicht nur zeitnäher und flexibler reagieren, sondern zugleich den erforderlichen Geheimnisschutz besser gewährleisten.

(3) Kontrolle durch Parlamentarische Ausschüsse

Die Kontrolle der amerikanischen Geheimdienste durch die dritte Gewalt wird durch die Parlamentsausschüsse des *Senate Judiciary Committee* (SJC), des *Senate Select Committee on Intelligence* (SSCI) und des *House Permanent Select Committee on Intelligence* (HPSCI) wahrgenommen.[404] Die beiden letztgenannten Gremien gingen Mitte der 70er Jahre aus dem *Church Committee* und dem *Pike Committee* hervor und vertreten die beiden Kammern des amerikanischen Kongresses. Das SSCI und das HPSCI sind als ständige Parlamentsausschüsse für die Budgetkontrolle sowie die allgemeine Überprüfung der geheimdienstlichen Aktivitäten und Überwachungsprogramme zuständig.[405] Das HPSCI ist spiegelbildlich zu den Mehrheitsverhältnissen des Repräsentantenhauses mit 18 Mitgliedern besetzt. Das SSCI besteht aus 17 Senatsmitgliedern ohne Berücksichtigung der Mehrheitsverhältnisse. Die zur Kontrolle erforderlichen Informationen erheben die Gremien zum Teil mittels eigener Ermittlungen oder Anhörungen.[406] Zudem sind der *Attorney General*, der Präsident, der DNI sowie die sonstigen Behördenleiter verpflichtet dem Kongress beziehungsweise den Gremien ausreichend und zeitnah über geplante und bedeutsame Geheimdienstaktivitäten zu berichten.[407] In diesem Zusammenhang müssen unter anderem rechtswidrige Überwachungsaktivitäten benannt werden.[408] Daneben ist das SJC als Rechtsausschuss des Senats zur Kontrolle des Justizministeriums und damit insbesondere zur Kontrolle des FBI berufen.[409] Aufgrund der Sensibilität der zur Verfügung gestellten Informationen müssen die

---

[403] Vgl. *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) ("A warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats"). Ebenso *Grunwald,* S. 113.

[404] Vgl. *Hörauf,* S. 298. Offizieller Internetauftritt http://intelligence.senate.gov/ und http://intelligence.house.gov/ [Stand: 1.5.2012].

[405] Vgl. *Hörauf,* S. 299; *Lundberg,* in: Baldino, S. 62, sowie zum SSCI http://intelligence.senate.gov/about.html [Stand: 1.5.2012]. Der HPSCI unterscheidet sich u.a. durch die Einbeziehung taktischer, d.h. mittelfristiger Erwägungen. Es ist zur Kontrolle des geheimdienstlichen Quellen- und Methodeneinsatzes befugt, vgl. *Hörauf,* S. 301.

[406] Vgl. *Hörauf,* S. 299.

[407] 50 U.S.C. §§ 413(a), 413a, 413b; §§ 1808, 1826, 1846.

[408] 50 U.S.C. § 413(b).

[409] Vgl. den offiziellen Auftritt unter http://www.judiciary.senate.gov/about/ [Stand: 1.5.2012]. Daneben verfügt auch das Repräsentantenhaus über einen Rechtsausschuss.

Gremien einen ausreichenden Geheimnisschutz gewährleisten können.[410] Schließlich existieren mit den sogenannten *Inspector Generals* weitere außerparlamentarische und unabhängige Kontrollinstanzen, die einem bestimmten Geheimdienst zugeordnet werden.[411] Sie kontrollieren intern sowohl die Effektivität, die Wirtschaftlichkeit als auch die Rechtmäßigkeit der Aufgabenwahrnehmung.[412] Zu diesem Zweck sind ihnen sämtliche Dienstunterlagen zugänglich zu machen.[413] Über die Ergebnisse werden der jeweilige Behördenleiter und der Kongress regelmäßig informiert.[414]

bb) Präventiv- beziehungsweise Vorabkontrolle

Die im Vorfeld einer Maßnahme greifenden Kontrollmechanismen unterscheiden sich nach der Erhebungsmethode, dem Einsatzort und dem Beobachtungsobjekt.

Die Mehrzahl der geheimdienstlichen Erhebungsmethoden unterliegt lediglich internen Vorabkontrollen, die sich beispielsweise in Aufsichtsbefugnissen des Behördenleiters oder bestimmten Antragserfordernissen niederschlagen können.[415] Ob diese internen Mechanismen durch eine richterliche Vorabkontrolle ergänzt werden, bestimmt sich danach, ob eine Maßnahme in den Anwendungsbereich des vierten Verfassungszusatzes fällt oder nicht. Außerhalb des vierten Verfassungszusatzes ist ein Richtervorbehalt selbst bei eingriffsintensiven Maßnahmen nicht vorgesehen.[416] Ein Beispiel sind etwa die *National Security Letters*.[417] Diese werden direkt von den Bundesbeamten erlassen, ohne dass eine Kontrolle durch eine gerichtliche Instanz zwischengeschaltet ist.[418]

Ist der Anwendungsbereich des vierten Verfassungszusatzes allerdings eröffnet, werden die Vorabkontrollen durch die Notwendigkeit eines *warrants* als richterliche Anordnung ergänzt. An das *warrant*-Erfordernis werden je nach Aufklärungsrichtung unterschiedliche Anforderungen gestellt, welche zudem durch unterschiedliche Gerichte geprüft werden. Für *domestic intelligence investigations* wur-

---

410 50 U.S.C. § 413(d), vgl. auch *Hörauf,* S. 300.

411 So etwa bei der CIA, vgl. dazu die offizielle Website https://www.cia.gov/about-cia/faqs/index.html#covertactions [Stand: 1.5.2012].

412 Grundlage bildet der reformierte *Inspector General Act* von 1978 (Pub. L. 111-259 vom 7.10.2010), vgl. www.ignet.gov/igs/faq1.html [Stand: 1.5.2012]; *Hörauf,* S. 303.

413 E.O. 12333 von 2008 unter Punkt 1.6.(h).

414 Vgl. www.ignet.gov/igs/faq1.html#mission [Stand: 1.5.2012], sowie *Hörauf,* S. 304, in Bezug auf die CIA.

415 Vgl. E.O. 12333 von 2008 unter Punkt 1.6 und Mukasey Guidelines 2008, II.A.2; II.B.2; II.B.5. Kritisch *Berman*, S. 54 Fn. 125.

416 Vgl. *Berman*, S. 22.

417 Vgl. *Grunwald,* S. 253.

418 Vgl. zur Anordnungskompetenz 18 U.S.C. § 2709(b); 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 50 U.S.C. § 436; vgl. insgesamt *Liu,* CRS 2011, S. 4.

de mit der bereits besprochenen *Keith*-Entscheidung die Notwendigkeit eines klassischen *warrants* festgeschrieben, sodass die Anordnungsbefugnis unverändert bei den Bundesgerichten liegt. Zwar wurde in diesem Urteil eine Absenkung der *probable cause*-Schwelle für möglich gehalten, durch den Verzicht eines dem FISA vergleichbaren *domestic warrant*-Regimes müssen sich *domestic intelligence* allerdings weiterhin auf einen klassischen *warrant* stützen können.[419] Der Erlass der richterlichen Anordnung steht zudem im Ermessen des jeweiligen Richters.[420]

Bei *foreign intelligence investigations* wird demgegenüber auf das Erfordernis eines klassischen *warrants* verzichtet und durch die spezifischen Kontrollmechanismen des FISA ersetzt. Die Durchführung einer FISA-Maßnahme bedarf im Regelfall einer Anordnung durch den FISC, die nach Ansicht der Rechtsprechung einem *warrant* hinreichend nahe kommt.[421] Antragsberechtigt sind lediglich Bundesbeamte, die sogenannten *federal officers*.[422] Die richterliche Überprüfung findet unter Ausschluss der Öffentlichkeit und des Beschuldigten und damit sowohl *in camera* als auch *ex parte* statt.[423] Die Kontrollmöglichkeiten der FISC-Richter sind wesentlich eingeschränkter als bei einer bundesgerichtlichen Kontrolle. Anders als bei Erlass eines klassischen *warrants* kann der Richter nicht nach eigenem Ermessen entscheiden, sondern ist grundsätzlich an die Einschätzungen der Beantragenden gebunden.[424] Dies wird bei einem Vergleich beider Regelwerke deutlich. Während der FISA in 50 U.S.C. § 1805(a)(2) von "shall enter an […] order" spricht, ist in 18 U.S.C. § 2518(3) des Title III lediglich von "may enter" die Rede.[425] Lediglich Maßnahmen gegen *U.S. Persons* dürfen auf grobe Fehler untersucht werden.[426] Durch diese Vorgaben wird der richterliche Kontrollrahmen auf willkürliche Entscheidungen und damit auf ein absolutes Minimum reduziert.[427]

---

[419] Dies gilt zumindest für elektronische Überwachungsmaßnahmen, die abseits der Ermächtigungen des Title III und des FISA nach 18 U.S.C. § 2511(2)(f) unzulässig sind. Da bei DII der erforderliche Auslandsbezug des FISA fehlt, muss auf die Voraussetzungen des Title III und damit auf das dort geltende *warrant*-Erfordernis zurückgegriffen werden; vgl. *Grunwald,* S. 72, 76; *Kerr,* Tex. L. Rev. (88) 2010, S. 1676.

[420] Siehe 18 U.S.C. § 2518(3). Vgl. zur Zuständigkeit und zum Verfahrensablauf FRCrimP Rule 41(b), (d)(2).

[421] Vgl. *In re Sealed Case*, 310 F.3d 717, 746 (FISCR 2002) "the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close".

[422] 50 U.S.C. § 1804(a); *Arzt,* in: Graulich/Simon, S. 258; *Hall,* Wake Forest L. Rev. (41) 2006, S. 74; *Kris,* in: Wittes, S. 220.

[423] 50 U.S.C. § 1805.

[424] Vgl. *United States v. Rahman*, 861 F. Supp. 247, 250f (S.D.N.Y. 1994). Darin heißt es: "it was not the function of that FISA court judge nor is it the function of this judge to 'second-guess' the certifications".

[425] Vgl. auch *Grunwald,* S. 108. 109.

[426] 50 U.S.C. § 1805(a)(4).

[427] Vgl. *Grunwald,* S. 109; *Rackow,* U. Pa. L. Rev. (150) 2002, S. 1681.

Aufgrund der begrenzten Einwirkungs- und Kontrollmöglichkeiten wird die Effektivität der Kontrolle durch den FISC zum Teil bezweifelt. Als erster Kritikpunkt wird die Informationsabhängigkeit der FISC-Richter angeführt. Ihnen fehle es oftmals an unabhängigen Erkenntnisquellen, um die vorgelegten Tatsachen hinreichend überprüfen zu können.[428] Aus diesem Grund würden FISA-Anträge fast zu einhundert Prozent bestätigt.[429] Zudem sei die bei *Non-U.S. Persons* auf bloße Verfahrensmängel und bei *U.S. Persons* auf offensichtliche Fehler beschränkte Prüfungskompetenz bedenklich. Durch diese inhaltliche Bindung werde letztlich die Entscheidungsbefugnis von den Gerichten auf die Exekutive verschoben.[430]

Zusätzlich zu den abgesenkten Kontrollstandards gestattet der FISA in bestimmten Ausnahmefällen sogar den vollständigen Verzicht auf eine FISA *order*. In diesen Fällen werden die Anordnungsbefugnis und damit die Verantwortung für die Überwachung allein dem *Attorney General* übertragen.[431] Eine solche Ausnahme ist neben dem Einsatz zu Übungszwecken[432] bei der Überwachung eines nur Ausländer erfassenden Sachverhalts, Eilfällen oder Maßnahmen in Kriegszeiten vorgesehen. Die besagte ausländerspezifische Ausnahmeregelung erfordert zunächst einen auf *official foreign powers* begrenzten Sachverhalt.[433] Hiervon werden beispielsweise ausländische Regierungen oder Regierungseinheiten, nationale Splittergruppen oder von ausländischen Regierungen offiziell anerkannte Organisationen erfasst.[434] Daneben muss die Involvierung einer *U.S. Person* weitgehend ausgeschlossen sein und die *minimization procedures* sind zu beachten.[435] In diesem Fall wird die Anordnungskompetenz auf den *Attorney General* in seiner Funktion als Bevollmächtigter des Präsidenten verlagert.[436] Der *Attorney General* muss seinerseits eine Erklärung beim FISC hinterlegen, in der er unter Eid das Vorliegen der

---

428 Vgl. *Standler*, S. 50.

429 Kritisch daher *Chiarella/Newton,* Army Law., 1997, S. 31; *Hardin,* Geo. Wash. L. Rev. (71) 2003, S. 337, 343; *Standler*, S. 25, 40, 50. Eine Übersicht der beantragten und abgelehnten FISA-Anträge im Zeitraum 1979 bis 2010 findet sich unter http://epic.org/privacy/wiretap/stats/fisa_stats.html [Stand: 1.5.2012]. Nach dem Jahresbericht vom 30.4.2013 hat der FISC im Kalenderjahr 2012 fast alle vorgelegten Anfragen bewilligt, siehe http://www.fas.org/irp/agency/doj/fisa/2012rept.pdf [Stand: 1.5.2013].

430 Vgl. *Evans,* Loy. U. Chi. L.J. (33) 2002, S. 974; *Hardin,* Geo. Wash. L. Rev. (71) 2003, S. 343. Zu den unterschiedlichen Standards bei *U.S. Persons* vgl. *Kris/Wilson,* § 32:5, S. 288.

431 Vgl. hierzu *Hall,* Wake Forest L. Rev. (41) 2006, S. 77ff. Zur Errichtung einer unabhängigen Stelle zur Ahndung von FISA-Verstößen vgl. *Standler*, S. 50.

432 Siehe 50 U.S.C. § 1805(f).

433 Vgl. 50 U.S.C. §§ 1802, 1822; *Hall,* Wake Forest L. Rev. (41) 2006, S. 78; *Kris/Wilson,* § 12:2.

434 50 U.S.C. § 1801(a)(1)–(3). Ein Beispiel ist die Palestine Liberation Organization. Nicht erfasst ist der internationale Terrorismus, vgl. *Kris/Wilson,* § 12:3, S. 447.

435 50 U.S.C. §§ 1802(a)(1)(B); 1822(a)(1)(A)(ii) sprechen von "no substantial likelihood"; vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 78.

436 50 U.S.C. § 1802. Längere Überwachungen bedürfen einer FISA-Anordnung.

genannten Anordnungsvoraussetzungen versichert *(certification requirement)*.[437] Eine nachträgliche Überprüfung dieser Versicherung durch den FISC erfolgt nicht.[438] Sie bleibt grundsätzlich unter Verschluss, es sei denn, die Regierung fordert die Offenlegung im Rahmen einer Rechtmäßigkeitskontrolle.[439] Noch geringere Voraussetzungen gelten bei einer Überwachungsmaßnahme von Ausländern im Ausland. Diese bedürfen nach 50 U.S.C. § 1881A(a) lediglich der Bevollmächtigung durch den *Attorney General* oder des CIA-Direktors.[440]

Die ebenfalls erwähnte Eilkompetenz erfordert demgegenüber eine Gefahrensituation, in der das Abwarten einer FISC-Anordnung den Erhalt von *foreign intelligence information* gefährden würde.[441] Im Gegensatz zur Eilkompetenz des Title III ist damit weder ein drohender Beweismittelverlust noch eine unmittelbar bevorstehende Lebensgefahr oder eine Bedrohung der nationalen Sicherheit erforderlich.[442] Hintergrund dieser unterschiedlichen Standards ist die abweichende Zwecksetzung des FISA, der die Erlangung von *foreign intelligence* in den Vordergrund stellt.[443] Für eine Überwachung genügt es, wenn der *Attorney General* von einer ausreichenden Tatsachengrundlage für eine Anordnung ausgeht und eine Bestätigung durch den FISC innerhalb von sieben Tagen nachholt.[444]

Viertens und letztens wird vom Erfordernis einer FISA-Anordnung in Kriegszeiten abgesehen.[445] In diesem Fall wird der *Attorney General* zum Erlass von Überwachungsmaßnahmen innerhalb einer 15-tägigen Frist nach erfolgter Kriegserklärung durch den Kongress ermächtigt. Diese Frist soll dem Kongress ausreichend Zeit für mögliche Ergänzungen des FISA geben.[446]

Der Kongress geht grundsätzlich vom abschließenden Charakter der dargestellten Ausnahmeregelungen aus.[447] Dem folgt die Regierungspraxis nicht, welche dem Präsidenten weiterhin die verfassungsrechtliche Befugnis zur Durchführung von geheimdienstlichen Überwachungsmaßnahmen ohne Bindung an einen Richter-

---

437 Vgl. hierzu *Arzt,* in: Graulich/Simon, S. 258.

438 Vgl. *Kris/Wilson,* § 12:2, S. 445.

439 Vgl. *Smith/Howe,* in: Markle Foundation, S. 140.

440 Daneben gilt für die elektronische Überwachung im Ausland die Richtlinie des U.S. Verteidigungsministeriums, Dir. 5240.1-R. Vertiefend *Chiarella/Newton,* Army Law. (25) 1997, S. 25. Bei *U.S. Persons* entscheidet allerdings der FISC, vgl. 50 U.S.C. § 1881B.

441 Vgl. 50 U.S.C. §§ 1805(e)(1)(A); vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 77.

442 18 U.S.C. § 2518(7)(a).

443 So *Kris/Wilson,* § 12:7, S. 457.

444 Zur elektronischen Überwachung 50 U.S.C. § 1805(e)(1)(B), (D); vgl. zudem § 1824(e) *(physical surveillance);* § 1843 *(pen/trap)*. Vgl. hierzu insgesamt *Kris/Wilson,* § 12:7.

445 50 U.S.C. §§ 1811, 1829.

446 Vgl. *Kris/Wilson,* § 12:8, S. 459.

447 So *Kris/Wilson,* § 12:1, S. 444.

vorbehalt zugesteht.[448] Auf dieser Grundlage wurden unter anderem Überwachungsprogramme wie das angesprochene *NSA-Surveillance Program* gestattet.[449] Entsprechend dieser Sonderbefugnis sind im amerikanischen Geheimdienstrecht daher weitere Überwachungsmaßnahmen denkbar, die vor ihrer Durchführung keiner gerichtlichen Vorabkontrolle zugeführt werden.

cc) Nachträgliche Kontrolle

Die nachträgliche Kontrolle des Geheimdienstsektors erfolgt vor allem durch parlamentarische Ausschüsse und Gerichte.

(1) Parlamentarische Kontrolle

Die parlamentarische Kontrolle wird primär mit Hilfe der bestehenden Berichtspflichten wahrgenommen. Diese wurden zum Teil bereits bei der Vorstellung der verschiedenen Kontrollinstanzen dargelegt. An dieser Stelle ist die dem *Attorney General* obliegende Informationspflicht hervorzuheben, wonach er die Rechtsausschüsse, das HPSCI und das SSCI halbjährlich über die Nutzung des FISA vollständig informieren muss.[450] Diese Berichte müssen unter anderem Angaben zur Anzahl der beantragten und durchgeführten Überwachungsmaßnahmen und Eilanordnungen sowie zur Häufigkeit der strafrechtlichen FISA-Nutzung enthalten.[451] Bei elektronischen Telekommunikationsüberwachungen muss der Kongress zudem jährlich über beantragte, verlängerte oder modifizierte elektronische Maßnahmen informiert werden.[452] In Bezug auf Durchsuchungsmaßnahmen oder andere elektronische Maßnahmen wurde überwiegend auf vergleichbare Pflichten verzichtet.[453]

(2) Gerichtliche Kontrolle

Die daneben bestehenden gerichtlichen Kontrollmöglichkeiten spielen vor allem unter Rechtsschutzgesichtspunkten eine zentrale Rolle. Die konkret zur Anwendung kommenden Kontrollstandards orientieren sich erneut an der Aufteilung in DII und FII. Dementsprechend unterliegt die nachträgliche Kontrolle rein inlandsbezogener Aufklärungsmaßnahmen dem für strafrechtliche Ermittlungen geltenden

---

[448] Vgl. *Kris/Wilson,* § 12:1, S. 444.

[449] Vgl. *Kris/Wilson,* § 15.

[450] Die 50 U.S.C. §§ 1808(a)(1), 1826; 1846(a), 1862(a) sprechen von "fully inform"; *Kris/Wilson,* § 13:2, S. 462.

[451] Vgl. 50 U.S.C. §§ 1808(a)(2)(A)–(C), 1826. Vertiefend *Kris/Wilson,* § 13:2.

[452] Siehe 50 U.S.C. § 1807, auch für Maßnahmen nach § 1862(c)(1),(2).

[453] Vgl. *Kris/Wilson,* § 13:3, S. 469.

Kontrollrahmen, während für Maßnahmen mit Auslandsbezug die Sonderregeln des FISA zur Anwendung kommen.

Letztere sehen im Vergleich zu den klassischen Rechtsschutzmöglichkeiten geringere nachträgliche Überprüfungsmöglichkeiten vor. Die Einschränkungen betreffen sowohl die laufenden als auch die nachträglichen Kontrollmöglichkeiten. Anders als Maßnahmen nach Title III werden FISA-Maßnahmen beispielsweise nicht bereits nach 30 Tagen, sondern erst nach 90 Tagen einer Nachprüfung unterzogen.[454] Ebenso verhält es sich in Bezug auf die jeweils geltende Pflicht, den Betroffenen von der Überwachung zu benachrichtigen. Während der Title III in 18 U.S.C. § 2518(8)(d) spätestens nach 90 Tagen eine Mitteilungspflicht vorsieht, unterliegen FISA-Überwachungen der Geheimhaltung.[455] Eine nachträgliche Kontrolle scheidet demgemäß in den meistens Fällen mangels Kenntnis aus.

Der Geheimnisschutz im FISA wird lediglich in drei Ausnahmefällen durchbrochen. Eine solche Ausnahme ist anzunehmen, wenn erstens die Regierung die Nutzung von FISA-Informationen gegen den Betroffenen beabsichtigt,[456] zweitens eine Eilmaßnahme nicht nachträglich durch den FISC bestätigt wurde[457] oder drittens das Geheimhaltungsinteresse weggefallen[458] ist. In diesen Fällen wird nicht nur der Betroffene, sondern zusätzlich das zuständige Gericht in Kenntnis gesetzt.[459] In der Folge können sowohl der Betroffene als auch die Regierung die Überwachungsmaßnahme nachträglich auf ihre Rechtmäßigkeit kontrollieren lassen.[460] Die Rechtsmäßigkeitskontrolle selbst wird einheitlich durch die zivilen Gerichte wahrgenommen; der FISC ist nicht zuständig. Da der *Attorney General* in den meisten Fällen in Bezug auf eine drohende Offenlegung die Gefährdung der nationalen Sicherheit unter Eid versichern wird, erfolgt die nachträgliche Überprüfung von FISA-Maßnahmen üblicherweise unter Ausschluss der Öffentlichkeit und des Betroffenen.[461] Eine Offenlegung der Materialien gegenüber dem Betroffenen

---

454 Vgl. *Rackow,* U. Pa. L. Rev. (150) 2002, S. 1681f.

455 Vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 69; *Kris/Wilson,* § 29:2, S. 227. Eine Verzögerung ist aber durch den *sneak and peek warrant* nach 18 U.S.C. § 3103a(b) möglich.

456 Siehe 50 U.S.C. §§ 1806(c), 1825(d), 1845(c). Bei einer elektronischen Überwachung ist eine Mitteilung nur erforderlich, wenn der Betroffene an der Kommunikation selbst beteiligt war. Dementsprechend fordert 50 U.S.C. § 1806(c) Informationen "derived from an electronic surveillance of that aggrieved person", vgl. *Kris/Wilson,* § 29:5, S. 235.

457 50 U.S.C. §§ 1806(j); 1825(j); vgl. *Kris/Wilson,* § 29:8–§ 29:10, S. 239ff.

458 Diese Ausnahme gilt nur bei Durchsuchungen nach 50 U.S.C. § 1825(b), vgl. *Kris/Wilson,* § 29:10, S. 241. Eine Ausweitung auf elektronische Überwachungsmaßnahmen fehlt trotz vergleichbarer Eingriffsintensität.

459 Das Gesetz spricht von "any court", sodass nicht der FISC gemeint ist, vgl. auch *Kris/Wilson,* § 30:1, S. 245.

460 Vgl. zur Auslösung der richterlichen Kontrolle *Kris/Wilson,* § 30:3, S. 246.

461 50 U.S.C. §§ 1806(f), 1825(g), 1845(f)(1). Die Versicherung selbst unterliegt keiner Geheimhaltung. Zum Teil wird diese Erklärung allerdings durch eine als geheim eingestufte Versicherung eines hochrangigen FBI-Beamten ergänzt, in der die Gründe für die Ge-

ist nur dann möglich, wenn dies zur Überprüfung der Rechtmäßigkeit der FISA-Maßnahme notwendig ist.[462]

Die Ausgestaltung des nachträglichen Rechtsschutzes wird aufgrund der speziell geregelten Zugangs- und Kontrollmöglichkeiten zum Teil sehr kritisch gesehen. Anknüpfungspunkt der Kritik ist die konkrete Ausgestaltung der Relevanz- und Zulässigkeitsprüfung. Da die richterliche Kontrolle aus Gründen der nationalen Sicherheit regelmäßig unter Ausschluss des Angeklagten erfolge, seien die Erfolgschancen einer Rechtmäßigkeitskontrolle relativ gering. Der Angeklagte könne mangels Zugang zu den FISA-Vorgängen den Vorwurf rechtswidrigen Handelns oftmals nur auf abstrakte beziehungsweise theoretische Mutmaßungen stützen, was in den meisten Fällen kaum Erfolg verspreche.[463] Zudem sei das Gericht in seiner Prüfungskompetenz durch die Einschätzungen der Exekutive bei Erlass der FISA-Anordnung gebunden, sodass sich die Kontrolle auf offensichtliche Fehler beschränke.[464] Da die Rechtmäßigkeitsentscheidung bindend sei, habe der Angeklagte in der Folge keine Möglichkeit, die Rechtmäßigkeit der Überwachung überprüfen zu lassen. Zudem verteile der FISA die Einwirkungsmöglichkeiten ungleich zulasten des Betroffenen.[465] Während die Regierung gegen eine Nichtzulassungsentscheidung Berufung einlegen kann, steht diese Möglichkeit dem Betroffenen nicht zu.[466]

dd) Zwischenergebnis zu Kontrollinstanzen

Die Kontrolle des amerikanischen Geheimdienstsektors orientiert sich erneut an der Aufteilung in *domestic* und *foreign intelligence investigations*. Daneben werden bei einer Überwachung von *U.S. Persons* und *Non-U.S. Persons* unterschiedliche Kontrollstandards angelegt.[467] Insgesamt erweisen sich die im FISA vorgesehenen gerichtlichen Kontrollmöglichkeiten als stark reduziert. Dies wird vor allem

---

heimhaltung dargelegt werden. Diese Erklärung ist selbst mit *security clearance* nicht einsehbar, vgl. *Kris/Wilson,* § 30:7, S. 254.

462 50 U.S.C. §§ 1806(f), 1825(g), 1845(f)(1).

463 Vgl. *Kris/Wilson,* § 32:2, S. 281. Zur Geheimhaltung aufgrund eines Antrags des *Attorney General* 50 U.S.C. § 1806(f); § 1825(g); § 1845 (f)(1), sowie vertiefend *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 154.

464 Vgl. *Kris/Wilson,* § 32:5, S. 288ff. Das überprüfende Gericht unterliegt damit ähnlichen Beschränkungen wie bereits der FISC im Rahmen der Anordnungskompetenz. Allerdings wird diese Begrenzung nicht von allen Gerichten eingehalten.

465 Nach 50 U.S.C. §§ 1806(g), 1825(h) besteht eine Pflicht, während nach 50 U.S.C. § 1845(g)(1) die Nichtzulassung im Ermessen des Gerichts steht. Die Feststellung der Rechtswidrigkeit ist nach der bisherigen Rechtsprechungspraxis relativ unwahrscheinlich; vgl. insgesamt *Hall,* Wake Forest L. Rev. (41) 2006, S. 70; *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 145.

466 Vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 70; *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 145.

467 Vgl. *Chiarella/Newton,* Army Law. (25) 1997, S. 30.

mit Blick auf die Anordnungskompetenzen des FISC und die beschränkten Zugangsmöglichkeiten im nachträglichen Rechtsschutz deutlich. Im Gegenzug verlagern sich die Kontrollkompetenzen auf interne beziehungsweise nachträgliche Verwaltungskontrollen und Berichtspflichten.

g) Zwischenergebnis zu den Besonderheiten geheimdienstlicher Ermittlungen

Die Besonderheiten geheimdienstlicher Ermittlungen werden maßgeblich durch die Einteilung in *domestic intelligence investigations* und *foreign intelligence investigations* bestimmt. Grund für diese Unterscheidung sind die erhöhten verfassungsrechtlichen Schutzstandards für rein inländische Beobachtungssubjekte. Da im Bereich der DII keine den Verfassungsvorgaben entsprechende Spezialermächtigung geschaffen wurde, unterliegen diese im verfassungsrelevanten Bereich den Anforderungen der strafrechtlichen Ermächtigungsgrundlagen; etwa dem dargestellten Title III.

Geheimdienstliche Ermittlungen mit Auslandsbezug sind demgegenüber an die Vorgaben des FISA gebunden. Dieser stellt in den meisten Fällen geringere Anforderungen und ermöglicht zugleich eine umfassendere Informationserhebung. Die Differenzierung zwischen Straf- und Geheimdienstrecht ist damit nur im Verhältnis zum FISA von Bedeutung. Die im FISA eingeräumten Befugnisse wurden allerdings durch dessen Öffnung verstärkt auch anderen Ermittlungszwecken zugänglich gemacht. Dies führt dazu, dass die Besonderheiten geheimdienstlicher Ermittlungen zwar weiterhin durch die Strukturvorgaben des vierten Verfassungszusatzes und der gerichtlich akzeptierten Sonderstellung der FII bestimmt werden, die ehemalige Unterscheidung faktisch jedoch an Bedeutung verliert. Darüber hinaus wurde deutlich, dass das amerikanische Geheimdienstrecht für Maßnahmen innerhalb der USA sowie generell gegenüber *U.S. Persons* weiterhin erhöhte Eingriffsvoraussetzungen und Kontrollstandards vorsieht.[468] Die geheimdienstliche Informationserhebung unterliegt damit je nach Einsatzort, Zielsetzung und Beobachtungssubjekt unterschiedlichen Standards.

2. Allgemeine Grenzen einer Informationsnutzung

Die Nutzung von Geheimdienstinformationen unterliegt allgemeinen Grenzen, die im Einzelnen durch die Gestaltung der Rechts- und Sicherheitsarchitektur bestimmt werden.

---

[468] Vgl. E.O. 12333 von 2008 unter Punkt 2.4; *Smith/Howe,* in: Markle Foundation, S. 134.

a) Grenzen aufgrund der Sicherheitsarchitektur

Die systembedingten Beschränkungen im Geheimdienstwesen wurden nach den Ereignissen von 2001 weitgehend aufgehoben. Die heutige Gestaltung der amerikanischen Sicherheitsarchitektur steht einem Wissensaustausch der verschiedenen Sicherheitsbehörden grundsätzlich offen gegenüber. Die für das Geheimdienstrecht zentrale E.O. 12333 von 2008 fordert sowohl den Austausch von Geheimdienstinformationen im Allgemeinen[469] als auch im Speziellen für die Auslands-, Spionage-, Drogen- und Terroraufklärung.[470] Zusätzlich werden Informationspflichten der einzelnen Geheimdienste sowie verschiedene Kooperationsformen und Teilnahmemöglichkeiten an Strafverfolgungsmaßnahmen im Bereich der Auslands-, Drogen- und Terrorismusaufklärung begründet.[471] Hierdurch wurde selbst die kompetenzrechtliche Differenzierung zwischen Ermittlungsbehörden auf Bundes- und Einzelstaatenebene erheblich abgeschwächt.

Die konkreten Anforderungen an die Zusammenarbeit richten sich im Grundsatz weiterhin nach der Kategorisierung in *domestic intelligence* (DI) einerseits und *foreign intelligence* (FI) andererseits. Die im Zuge der rein inlandsbezogenen Aufklärung (DII) erhobenen Erkenntnisse können aufgrund der parallel verlaufenden Ermittlungsbefugnisse ohne weitere Voraussetzungen und unabhängig vom Erhebungskontext ausgetauscht und genutzt werden. Dieser Gleichlauf erklärt zugleich, warum der Wissensaustausch in diesem Bereich kaum als Problem wahrgenommen wird. Die Übermittlung ist an keine Pflicht gebunden, sondern erfolgt, sobald der zuständige Beamte von einer entsprechenden Notwendigkeit ausgeht.[472] Diese Schrankenlosigkeit wird vor allem am hybriden Charakter des FBI deutlich. Die Ermittlungsmaßnahmen werden dort einheitlich von einer Behörde wahrgenommen und können daher fließend von der Wahrnehmung nachrichtendienstlicher Tätigkeiten in die Strafverfolgung übergehen.[473] Die jeweiligen Erkenntnisse können letztlich direkt strafrechtlichen Zwecken zugeführt werden.[474] Aufgrund der konkreten Gestaltung des Sicherheitswesens unterliegen Erkenntnisse der DII damit

---

469 E.O. 12333 von 2008 unter Punkt 1.4.(c): "Consistent with applicable Federal law […] the Intelligence Community shall […] analyze, produce, and disseminate intelligence."

470 E.O. 12333 von 2008 unter Punkt 2.3.(c): "Those procedures shall permit […] dissemination of […] information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation."

471 E.O. 12333 von 2008 unter Punkt 1.7, 2.6: "participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities".

472 Vgl. die Mukasey Guidelines 2008 unter Punkt VI.B.1.a: "the FBI may disseminate information obtained or produced through activities under these Guidelines […] within the FBI and to other components of the Department of Justice".

473 Vgl. *Droste,* Nachrichtendienste, S. 84; *Hulnick,* IJIC (22) 2009, S. 579.

474 Vgl. *Hulnick,* IJIC (22) 2009, S. 579.

weder speziellen Übermittlungs- noch speziellen Nutzungsgrenzen. Dieses Konzept war zum Teil bereits vor den Änderungen von 2001 angelegt.

Die strafrechtliche Nutzung von Erkenntnissen der auslandsbezogenen Aufklärung (FII) war bis zu dem Erlass des *USA PATRIOT Act* demgegenüber nur beschränkt möglich. Die umfassende Abschottung zu anderen Sicherheitsbereichen wurde insofern als Rechtfertigung für die abgesenkten Schutzmechanismen angesehen. Für die CIA kam diese Abschottung im Inlandsvorbehalt zum Ausdruck, während im Anwendungsbereich des FISA die Nutzung von FISA-Erkenntnissen durch die sogenannte *wall* begrenzt wurde. Beide Grenzlinien wurden durch die Reformen nach 2001 abgeschwächt oder sogar aufgehoben. Der für die auslandsbezogene Inlandsaufklärung nach dem FISA bestehende *primary purpose*-Test wurde zugunsten einer *information sharing environment* ersetzt. Der seitdem für die Nutzung von FISA-Erkenntnissen bestehende *significant purpose*-Standard entfaltet nur noch in wenigen Ausnahmefällen eine limitierende Wirkung. Dies gilt in ähnlicher Weise für den angeführten Inlandsvorbehalt der CIA. Dieser Vorbehalt wurde in den einschlägigen Gesetzen aufrechterhalten, ohne ihn allerdings als eindeutiges und vollständiges Verbot zu präzisieren.[475] Die zumeist vage Formulierung des Inlandsvorbehalts konnte daher von den Gerichten seit jeher zugunsten einer begrenzten Inlandsaktivität ausgelegt werden. Dementsprechend finden sich in einzelnen Urteilen Formulierungen wie: "the Agency must, at times, pursue domestically its foreign intelligence mandate".[476] In gleicher Weise wird festgestellt: "the CIA can and does use domestic sources for foreign intelligence activities".[477] Da die Gerichte ihrerseits auf eine weitere Präzisierung der zulässigen Inlandsaktivitäten verzichteten, wurde die zulässige Grenze bis zum Jahr 2001 durch den sogenannten *principal purpose*-Test bestimmt.[478] Diese dem *primary purpose*-Standard sehr ähnliche Regelung gestattete eine Kooperation mit dem Strafverfolgungssektor, solange der Hauptschwerpunkt der Maßnahmen im Bereich der Auslands- und Spionageaufklärung lag.[479] Diese Beschränkung wurde mit den bereits angesprochenen Reformen zumindest in Bezug auf die Terrorbekämpfung hinfällig.[480] In der Gesamtschau führten die Reformbewegungen nach 2001 damit zu einer Neudefinition der amerikanischen Sicherheitsarchitektur, die dem Austausch

---

[475] Vgl. zur vagen Formulierung *Harris,* Yale L. & Pol'y Rev. (23) 2005, S. 533; *Hörauf,* S. 291; *Ortiz,* in: Markle Foundation, S. 95. Eine Ausnahme bildet die Telekommunikationsüberwachung.

[476] Siehe *Fitzgibbon v. CIA*, 911 F.2d 755, 764 (D.C. Cir. 1990).

[477] Siehe *Sirota v. CIA*, 1981 WL 158804, 1, 8 (S.D.N.Y. 1981); vgl. zudem *Harris,* Yale L. & Pol'y Rev. (23) 2005, S. 534. Die Einschränkung findet sich in E.O. 12333 von 2008 unter Punkt 2.4(a).

[478] Vgl. *Kris/Wilson,* § 2:11, S. 67f.

[479] Vgl. *Kris/Wilson,* § 2:11, S. 67.

[480] So *Hitz,* Harv. J. L. & Pub. Pol'y (25) 2002, S. 772f.

und der Nutzung von Geheimdienstinformationen kaum noch Hindernisse in den Weg stellt.

b) Grenze aufgrund der Rechte des Betroffenen

Ungeachtet der systembedingten Besonderheiten kann die Informationserhebung und -nutzung durch die Rechte des Betroffenen limitiert werden. Die hierdurch bedingten Beschränkungen werden vorliegend anhand der Garantien des ersten und vierten Verfassungszusatzes sowie den Vorschriften des *Privacy Act* von 1974 besprochen.

Der erste Verfassungszusatz schützt vor allem die Religions-, Rede-, Presse- und Versammlungsfreiheit.[481] Dieser Schutzanspruch wird in den meisten geheimdienstlichen Ermächtigungsgrundlagen berücksichtigt. Danach muss beispielsweise die Beobachtung einer *U.S. Person* unterbleiben, sofern die Überwachung ausschließlich erfolgen soll, weil diese die im ersten Verfassungszusatz verbürgten Rechte wahrnimmt. Der Bürger soll von der Wahrnehmung seiner Rechte nicht durch die staatliche Informationserhebung abgeschreckt werden.[482] Die gerichtliche Rüge dieser als *chilling effect* bezeichneten Abschreckungswirkung erfordert über das subjektive Empfinden hinaus allerdings eine objektiv feststellbare, nicht nur beiläufige Beeinträchtigung.[483]

Eine weitere Hürde ergibt sich aus den Garantien des vierten Verfassungszusatzes. Dieser schützt unter anderem das Vertrauen in den Schutz der Privatsphäre vor staatlichen Eingriffen.[484] Werden die dort genannten Vorgaben missachtet, führt dies grundsätzlich zur Unverwertbarkeit der erhobenen Erkenntnisse. Hierdurch werden der Informationserhebung und -nutzung zunächst erhebliche Grenzen gesetzt. Der mit der Verfassungsgarantie verbundene Schutz wird allerdings in mehrfacher Hinsicht relativiert. Zum einen ist der Anwendungsbereich des vierten Verfassungszusatzes auf den Schutz sogenannter *search and seizure*-Maßnahmen und damit inhaltlich auf bestimmte Fälle zugeschnitten.[485] Zum anderen werden die tatsächlichen Anwendungsfälle durch Vorgaben der Rechtsprechung erheblich minimiert. In diesem Zusammenhang wurde unter anderem die Vereinbarkeit der FISA *order* mit den Vorgaben des vierten Verfassungszusatzes mehrfach bestä-

---

[481] Vgl. *Grunwald,* S. 59; *Thompson/Nored/Worrall/Hemmens,* S. 10f.

[482] Vgl. hierzu *Grunwald,* S. 59.

[483] Vgl. *Laird v. Tatum,* 408 U.S. 1, 14 (S. Ct. 1972): "Allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm"; vgl *Grunwald,* S. 61. Andernfalls ist das erforderliche *standing* zu verneinen.

[484] Vgl. *Genz,* S. 45.

[485] So *Genz,* S. 47.

tigt.[486] Die Anordnung durch den FISC käme insofern einem *warrant* im klassischen Sinne hinreichend nahe, obwohl dieser anderen Verfahrensregeln und Standards unterliege.[487] Zusätzlich zu dieser Sonderregel werden einzelne Daten aus dem Schutzbereich des vierten Verfassungszusatzes herausgenommen. Eine derart zentrale Ausnahme betrifft den Schutz von Daten, die zu ihrer Speicherung dritten Personen zugänglich gemacht werden. Durch diese Zugänglichmachung verlieren die Daten nach Ansicht der Rechtsprechung ihren privaten Charakter und damit den Schutz des vierten Verfassungszusatzes.[488] Dieses Verständnis führt dazu, dass etwa Bankunterlagen nicht als private Dokumente, sondern als Geschäftsunterlagen der Bank behandelt werden, deren Weitergabe der Betroffene an die Regierung in Kauf nehme.[489] Das Fehlen eines schutzwürdigen Vertrauens wird ebenfalls als Argumentation für die abgesenkten Anforderungen an die Herausgabe von Geschäftsunterlagen nach 50 U.S.C. §§ 1861ff angeführt.[490] Selbst der zum Schutz von Finanz- und Kontoinformationen geschaffene *Right to Financial Privacy Act* führt zu keinem anderen Ergebnis, da geheimdienstliche Überwachungen ausdrücklich von den gesetzlichen Beschränkungen ausgenommen wurden.[491] Diese Ausnahme wird aufgrund der vermehrten Auslagerung von Speichermöglichkeiten für zukünftige Ermittlungen an Bedeutung gewinnen.[492] Eine zweite Ausnahme betrifft Fälle, in denen eine der überwachten Personen in die Überwachung eingewilligt hat.[493] Diese Konstellation fällt mangels Vertrauensschutz ebenfalls aus dem Anwendungsbereich des vierten Verfassungszusatzes heraus. Nach der Rechtsprechung werde mit der Offenbarung gegenüber einer dritten Person bewusst das Risiko einer Informationsweitergabe eingegangen. Eine dritte Ausnahme betrifft den Schutz von sogenannten Verbindungsdaten, bei denen es ebenfalls an einem

---

[486] Vgl. vor 2001 *United States v. Nicholson*, 955 F.Supp. 588, 590 (E.D.Va. 1997) sowie *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); *United States v. Ning Wen*, 477 F.3d 896, 897ff (7th Cir. 2007). Einzige Ausnahme bildet die *Mayfield v. United States,* 504 F. Supp.2d 1023, 1036-43 (D.Or. 2007), die aber durch die Rechtsmittelentscheidungen *Mayfield v. United States*, 588 F.3d 1252 (9th Cir. 2009) und *Mayfield v. United States*, 599 F.3d 964 (9th Cir. 2010) aufgehoben wurde.

[487] Vgl. bereits Teil 3, III.B.1.f)bb) unter Verweis auf *In re Sealed Case*, 310 F.3d 717, 746 (FISCR 2002).

[488] Vgl. *Schwartz,* Hastings L.J. (54) 2003, S. 765.

[489] Vgl. *United States v. Miller*, 425 U.S. 435, 440, 443 (S. Ct. 1976): "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."

[490] Vgl. die unterschiedlichen Standards in 18 U.S.C. § 2511 für *wire and electronic communication* und § 2703 für *stored wire and electronic communication.*

[491] Nach 12 U.S.C. § 3406 ist eine Weitergabe an eine richterliche Anordnung gebunden, wovon geheimdienstliche Erhebungsmaßnahmen nach 12 U.S.C. § 3414 allerdings ausdrücklich ausgenommen sind, vgl. *Grunwald,* S. 214.

[492] Vgl. *Schwartz,* Hastings L.J. (54) 2003, S. 769; *Solove,* S. Cal. L. Rev. (75) 2002, S. 1089.

[493] Vgl. *Schwartz,* Hastings L.J. (54) 2003, S. 766.

schutzwürdigen Vertrauen fehle.[494] Anders als bei Inhaltsdaten bestehe in die Privatheit gewählter Rufnummern kein erkennbares oder nachvollziehbares Vertrauen. Diese Ausnahmen verdeutlichen den nur fragmentarischen Schutz des vierten Verfassungszusatzes. Ein allgemeiner verfassungsrechtlich verbürgter Schutz von Persönlichkeitsrechten beziehungsweise personenbezogenen Daten besteht nicht. Vielmehr werden die Schutzstandards in vereinzelten Gesetzen und Urteilen festgelegt.[495]

Zum Schutz vor einer ausufernden staatlichen Datensammlung und -verarbeitung wurde daher zumindest auf einfachgesetzlicher Ebene der *Privacy Act* von 1974 geschaffen.[496] Dieses Gesetz ist eine Reaktion auf die mit der Watergate Affäre aufgedeckten Missstände, in denen die Nixon Administration versucht hatte ihre politischen Gegner durch eine umfassende Datenerhebung auszuspionieren.[497] Die Vorgaben des *Privacy Act* sollten die Datensammlung und -speicherung auf das für die Aufgabenerfüllung erforderlich Maß reduzieren und eine Weitergabe personenbezogener Daten nur bei einer Einwilligung des Betroffenen gestatten.[498] Von dieser Grundregel wurden jedoch Schritt für Schritt zahlreiche Ausnahmen gemacht.[499] Im vorliegend relevanten Bereich ist eine Weitergabe und Offenlegung beispielsweise nach der *routine use exception* oder der *law enforcement exception* möglich. Die *routine use exception* gestattet die Weitergabe, wenn der ursprüngliche Erhebungszweck mit dem späteren Verwendungszweck vereinbar ist.[500] Da seit der Änderung des FISA geheimdienstliche und strafrechtliche Zwecke gleichzeitig verfolgt werden können, ist eine Weitergabe von FISA-Erkenntnissen fast beliebig möglich.[501] Daneben gestattet die *law enforcement exception* die Weitergabe zu Zwecken der Strafverfolgung. Für einen Austausch von Geheimdienstinformationen genügt bereits die Angabe der gewünschten Informationen und des späteren Verwendungszwecks.[502] Ausgeschlossen sind lediglich pauschale Anfragen einer nicht zur Strafverfolgung autorisierten Behörde. Die einschränkende Wirkung des Gesetzes wird zusätzlich dadurch reduziert, dass es nur auf Bundes-

---

494 Vgl. *Smith v. Maryland*, 442 U.S. 735, 741 (1979); *Schwartz,* Hastings L.J. (54) 2003, S. 768. Diese Ausnahme erklärt die für *pen/trap*-Maßnahmen abgesenkten Voraussetzungen.

495 Vgl. *Genz,* S. 39, 44.

496 Vgl. hierzu jeweils 5 U.S.C. § 552a zur Erhebung unter § 552a(e) i.V.m. (a)(3), zur Speicherung § 552a(c) und zur Weitergabe § 552a(b) sowie *Grunwald,* S. 184; *Solove,* S. Cal. L. Rev. (75) 2002, S. 1166.

497 Vgl. *Genz,* S. 51.

498 Vgl. 5 U.S.C. § 552a(e)(1), (b) sowie *Genz,* S. 50f.

499 Vgl. *Solove,* S. Cal. L. Rev. (75) 2002, S. 1166.

500 Siehe 5 U.S.C. § 552a(b)(3) i.V.m.(a)(7) i.V.m.(e)(4): "for a purpose which is compatible with the purpose for which it was collected"; vgl. *Grunwald,* S. 195.

501 Vgl. *Grunwald,* S. 195f. Formal ist der Zweck im Federal Register anzugeben.

502 Siehe U.S.C. § 552a(b)(7): "a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought"; vgl. *Grunwald,* S. 196f.

behörden anwendbar ist.[503] Auf Staatenebene wurde in mehr als der Hälfte der Staaten auf die Schaffung vergleichbarer Vorschriften verzichtet. Darüber hinaus werden zahlreiche Datenbanken explizit von den Regularien des *Privacy Act* befreit.[504] Der Informationsaustausch zwischen den Geheimdiensten und den Strafverfolgungsbehörden wird durch den *Privacy Act* damit nur geringfügig reguliert.

c) Zwischenergebnis zu Grenzen

Die Untersuchung der allgemeinen Grenzen einer Nutzung von Geheimdienstinformationen hat verdeutlicht, dass weder die amerikanische Sicherheitsarchitektur noch die Rechte des Betroffenen einer Verarbeitung personenbezogener Daten generell im Wege stehen. Eine Einschränkung erfolgt lediglich für vereinzelte Bereiche, sodass im Grundsatz die Nutzung geheimdienstlicher Erkenntnisse erlaubt ist.

3. Übermittlung von Geheimdienstinformationen

Geheimdienstinformationen können auf unterschiedlichen Wegen an die Strafverfolgungsbehörden beziehungsweise in ein Strafverfahren gelangen. Der grundsätzlich schrankenlose Datenaustausch steht allerdings unter dem Vorbehalt abweichender gesetzlicher Regeln beziehungsweise interner Richtlinien.[505] Deren explizite Ausgestaltung ist Gegenstand der nachfolgenden Ausführungen.

a) Eigenständige Übermittlung durch die Dienste

Geheimdienstinformationen können den Strafverfolgungsbehörden durch eine direkte Informationsübermittlung zugänglich gemacht werden.

aa) Übermittlungen nach den Mukasey Guidelines

Im Bereich der rein inlandsbezogenen Aufklärung (DII) werden die Anforderungen an einen Informationsaustausch primär durch die Mukasey Guidelines festgelegt. Die dortigen Übermittlungsvorschriften differenzieren danach, ob die entdeckte Straftat in die Verfolgungskompetenz des Bundes oder der Einzelstaaten fällt. Liegen konkrete Anhaltspunkte für die Verletzung des Bundesstrafrechts vor, greift die Übermittlungsvorschrift unter Punkt VI.C.1. der Mukasey Guidelines. Danach sind die Ermittlungsbeamten zu einer Kontaktaufnahme mit der zuständigen

---

503 Vgl. *Genz,* S. 51.

504 Insgesamt vertiefend *Grunwald,* S. 198f*; Solove,* S. Cal. L. Rev. (75) 2002, S. 1166.

505 Vgl. E.O. 12333 von 2008 unter Punkt 2.6: "Unless otherwise precluded by law or this Order".

Bundesstaatsanwaltschaft verpflichtet.[506] Taugliche Empfangsstelle ist unter anderem der *U.S. Attorney* oder ein Beamter des Justizministeriums. Voraussetzung einer Übermittlung und der damit einhergehenden Übermittlungspflicht ist das Vorliegen relevanter Tatsachen, die aller Wahrscheinlichkeit nach Strafverfolgungsmaßnahmen rechtfertigen.[507] Die Erkenntnisse müssen sich daher zu einem gewissen Grad verdichtet haben.[508] Bei strafrechtlich relevanten Vorgängen außerhalb der Bundeszuständigkeit greift die Übermittlungsvorschrift unter Punkt VI.C.2. der Mukasey Guidelines. Die erhobenen Erkenntnisse müssen in diesem Fall ebenfalls an die jeweils zuständige Strafverfolgungsbehörde übermittelt werden.[509] Voraussetzung ist das Bestehen glaubwürdiger Informationen in Bezug auf eine schwere kriminelle Handlung. Ausnahmsweise dürfen die FBI-Beamten von einer Übermittlung absehen, wenn sie sonst eigene Ermittlungen oder die Sicherheit von Personen und Quellen gefährden würden. Die zuständigen Behörden müssen allerdings so bald wie möglich über die besagten Informationen in Kenntnis gesetzt werden. Spätestens nach Ablauf einer 180-tägigen Frist ist die FBI-Hauptverwaltung schriftlich und regelmäßig über die Umstände und Gründe der Geheimhaltung zu informieren. Die Mukasey Guidelines begründen damit einheitlich eine Übermittlungspflicht, ohne die Informationsweitergabe selbst an weitere materielle Voraussetzungen zu knüpfen. Lediglich bei einer Übermittlung an die Strafverfolgungsbehörden der Einzelstaaten wird allgemein das Vorliegen einer schweren Straftat gefordert. Eine Präzisierung durch einen Straftatkatalog erfolgt nicht.

Diese Vorgaben sind weitgehend auf die Übermittlung von Erkenntnissen der National Security Letters übertragbar.[510] Eine Übermittlung zu Strafverfolgungszwecken ist damit grundsätzlich ohne weitere Voraussetzungen möglich.[511] Lediglich im Anwendungsbereich der 18 U.S.C. § 2709(d) und 12 U.S.C. § 3414(a)(5)(B) wird über die Anforderungen der Mukasey Guidelines hinaus zusätzlich eine klare Rele-

---

[506] Mukasey Guidelines, Punkt VI.C.1.: "shall maintain periodic written or oral contact with the appropriate federal prosecutor"; vgl. auch http://www.fbi.gov/about-us/faqs [Stand: 1.5.2012].

[507] Mukasey Guidelines, Punkt VI.C.1.: "When […] a matter appears arguably to warrant prosecution the agent shall present the relevant facts to the appropriate federal prosecutor." Konkret zum internen Ablauf vgl. *Rozen,* in: Markle Foundation, S. 117.

[508] Vgl. *Droste,* Nachrichtendienste, S. 84.

[509] Mukasey Guidelines Punkt VI.C.2.: "When credible information is received by an FBI field office concerning serious criminal activity not within the FBI's investigative jurisdiction, the field office shall promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction."

[510] Vgl. hierzu insgesamt *Doyle,* CRS 2011, S. 10; *Kris/Wilson,* § 20:9. Einzige Ausnahme bildet insofern die systemwidrige Begrenzung in 15 U.S.C. § 1681u, die vorliegend mangels Relevanz außer Betracht bleibt.

[511] So enthält 15 U.S.C. § 1681v keine weiteren Voraussetzungen. Bei 50 U.S.C. § 436 genügen Zwecke der Strafverfolgung.

vanz für den Verantwortungsbereich der Empfangsbehörde gefordert. Diese Bedingung wird man bei einer Übermittlung strafrechtlich relevanter Erkenntnisse an die Staatsanwaltschaft stets bejahen können.

bb) Übermittlungen nach dem FISA

Da im Bereich der Auslandsaufklärung erweiterte Erhebungsbefugnisse zur Verfügung stehen, soll eine schrankenlose Heranziehung von FISA-Material in Strafverfahren verhindert werden.[512] Dessen Übermittlung ist daher an zusätzliche Voraussetzungen gebunden.

Im Einzelnen sieht der FISA vier Voraussetzungen vor, die bei einer Übermittlung und Nutzung von FISA-Erkenntnissen zu Strafverfolgungszwecken zu beachten sind:[513] erstens die Einhaltung der sogenannten *minimization procedures*; zweitens das Vorliegen eines rechtmäßigen Zwecks; drittens die Genehmigung des Justizministers und viertens die Beachtung bestehender Sonderrechte. Je nach einschlägiger Ermittlungsmethode sind alle oder nur einzelne dieser Voraussetzungen zu beachten. Daneben ist eine Übermittlung möglich, wenn der Betroffene einwilligt. Einen Überblick über die bei den einzelnen Ermittlungsmethoden jeweils einzuhaltenden Anforderungen gibt Tabelle 2. Diese werden anschließend im Detail besprochen.

(1) Einhaltung der *minimization procedures*

Erste Voraussetzung einer Übermittlung von FISA-Erkenntnissen ist die Einhaltung der sogenannten *minimization procedures.* Hierbei handelt es sich um Verfahrensregeln, die einen angemessenen Ausgleich zwischen den staatlichen Interessen der Auslandsaufklärung und den Privatschutzinteressen des Einzelnen gewährleisten sollen.[514] Sie werden vom *Attorney General* individuell für die einzelnen Überwachungsmethoden erlassen und können bei Bedarf vom FISC modifiziert werden.[515] Da die *minimization procedures* weitgehend der Geheimhaltung unterliegen, kann nachfolgend allein auf die gesetzlichen Bestimmungen eingegangen werden.[516] Bei einer näheren Untersuchung der an die *minimization procedures* gesetzlich zu stellenden Mindestanforderung wird deutlich, dass diese sprachlich

---

[512] Vgl. *Arzt,* in: Graulich/Simon, S. 257.

[513] Vgl. *Kris/Wilson,* § 28:1, S. 205.

[514] Zur Erforderlichkeit der *minimization procedures* vgl. 50 U.S.C. §§1806(a) *(electronic surveillance)*, 1825(a) *(physical search)*, 1861(h) *(tangible things)*. Auf Verbindungsdaten finden die *minimization procedures* keine Anwendung. Zur Definition der *minimization procedures* vgl. 50 U.S.C. §§ 1801(h), 1821(4), 1861(g); vgl. hierzu ausführlich *Kris/Wilson,* § 9.

[515] Vgl. *Kris/Wilson,* § 9:1, S. 322.

[516] Zur grundsätzlichen Geheimhaltung vgl. *Kris,* in: Wittes, S. 219.

50 U.S.C.	Electronic surveillance	Physical search	Pen/Trap	Tangible things
Minimization procedures	§ 1806(a)	§ 1825(a)	–	§ 1861(h)
Rechtmäßiger Zweck	§ 1806(a)	§ 1825(a)	§ 1845(a)	§ 1861(h)
Genehmigung	§ 1806(b)	§ 1825(c)	§ 1845(b)	–
Erhalt von Privilegien	§ 1806(a)	–	–	§ 1861(h)

Tabelle 2

zwischen der Informationsverbreitung *(dissemination)*[517] einerseits und der Informationsnutzung und -offenlegung *(use and disclosure)*[518] andererseits unterscheiden. Bei einer ausschließlich am Wortlaut orientierten Auslegung könnte man geneigt sein die *dissemination* auf die rein interne Informationsnutzung und die *disclosure* auf die externe Weitergabe, etwa an einzelstaatliche und ausländische Behörden zu beziehen. Allerdings wird der sprachlichen Differenzierung keine inhaltliche Bedeutung beigemessen. Vielmehr werden die Verfahrensregeln auf jede Art von Weitergabe angewendet, unabhängig davon, ob diese an Behörden auf Bundes- oder Staatenebene erfolgt.[519] Damit sind die *minimization procedures* neben der Sammlung und Speicherung uneingeschränkt auf die vorliegend relevante Informationsweitergabe an die Staatsanwaltschaft anwendbar.

Inhaltlich untersagen die *minimization procedures* grundsätzlich jede Informationsübermittlung, die eine *U.S. Person* betreffen oder identifizieren kann.[520] Der Schutz der Verfahrensregeln ist hier ausschließlich auf *U.S. Persons* begrenzt.[521] Von diesem Weitergabeverbot wird allerdings bei strafrechtlich relevanten Sachverhalten eine Ausnahme gemacht.[522] Danach ist ein Austausch gestattet, wenn die Informationen als Beweismittel für ein begangenes oder künftiges Verbrechen zu Strafverfolgungszwecken herangezogen werden sollen.[523] Eine solche ausdrückliche Ausnahme ist nur im Bereich der normalen Kriminalität erforderlich. Auf die bereits bekannten *foreign intelligence crimes* findet das Weitergabeverbot entgegen dem missverständlichen Wortlaut der *minimization procedures* keine Anwen-

---

517 So in den 50 U.S.C. §§ 1806(a), 1825(a); 1861(h).

518 So in den 50 U.S.C. §§ 1801(h), 1821(4), 1861(g).

519 Vgl. *Kris/Wilson,* § 28:4, S. 215.

520 Vgl. 50 U.S.C. § 1801(h)(1), (2).

521 Vgl. *Kris/Wilson,* § 11:10, S. 414.

522 Vgl. *Grunwald,* S. 82.

523 Die 50 U.S.C. §§ 1801(h)(3), 1821(4)(C), 1861(g)(2)(C) gestatten "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed" zu "law enforcement purposes".

dung.[524] Die entsprechende Weitergabebefugnis folgt vielmehr bereits aus der Zielsetzung des FISA, der die Strafverfolgung als taugliches Instrument zur Herstellung der nationalen Sicherheit anerkennt. In diesem Sinne hat die bereits erläuterte Entscheidung des FISCR von 2002 die gezielte Erhebung von Erkenntnissen über den Begriff der *foreign intelligence crimes* gestattet.[525] Ausdrücklich untersagt wurde lediglich die Heranziehung des FISA zur ausschließlichen Aufklärung gewöhnlicher Kriminalität.[526] Erkenntnisse zu *foreign intelligence crimes* können demgegenüber sowohl zu geheimdienstlichen als auch zu strafrechtlichen Zwecken weitergegeben werden. Wird beispielsweise ein ausländischer Spion rechtmäßig nach dem FISA überwacht, darf das FBI die erhobenen Erkenntnisse sowohl der CIA als auch der Staatsanwaltschaft zur Verfügung zu stellen.[527] Während die CIA diese Erkenntnisse zum Beispiel zur Abwerbung des Spions oder zur Durchführung von *covert actions* nutzen wird, kann die Staatsanwaltschaft mit denselben Erkenntnissen beispielsweise ein Strafverfahren wegen Wirtschaftsspionage nach 18 U.S.C. § 1831 vorantreiben. Im Bereich der normalen Kriminalität lässt sich die Weitergabebefugnis demgegenüber gerade nicht aus der Zielsetzung des Gesetzes ableiten.[528] Diese Lücke wird durch die *minimization procedures* in den 50 U.S.C. §§ 1801(h)(3), 1821(4)(C), 1861(g)(2)(C) geschlossen, die ihrerseits eine Übermittlungsbefugnis für zufällig angefallene, strafrechtlich relevante Informationen statuieren.[529] Zur Verdeutlichung kann an das vorgenannte Beispiel angeknüpft werden. Wird bei der Überwachung des ausländischen Agenten dessen Sohn bei einem Autodiebstahl beobachtet, können diese Erkenntnisse der Staatsanwaltschaft übermittelt werden.[530] Eine ausschließliche Überwachung des Sohns auf der Grundlage des FISA wäre für sich gesehen zwar unzulässig gewesen, die zufällig angefallenen Erkenntnisse dürfen aufgrund der rechtmäßigen FISA-Überwachung dennoch übermittelt werden. Eine entsprechende Konstellation ergab sich bei einer in den 1990er Jahren durchgeführten Überwachung von Mitgliedern der Palästinensischen Befreiungsorganisation.[531] Im Verlauf der Observationen wurde bekannt, dass die überwachten Eheleute ihre Tochter umgebracht hatten. Obwohl diese Tat in keiner

---

[524] Erfasst werden Delikte des internationalen Terrorismus oder der Spionage; vgl. Teil 3, III.A.2. sowie die Aufzählung in 50 U.S.C. § 1801. Der dortige Wortlaut suggeriert, dass eine Weitergabe ohne Einhaltung der Verfahrensregeln grundsätzlich unzulässig ist. 50 U.S.C. §§1806(a) lautet: "information acquired […] may be used […] *only* in accordance with the minimization procedures" [Hervorhebung von Autorin]. Vgl. ebenfalls zu dieser Formulierung *Kris/Wilson,* § 28:2, S. 207.

[525] *In re Sealed Case*, 310 F. 3d, 717, 735; vgl. zudem *Kris/Wilson,* § 10:14, S. 385.

[526] Vgl. *Kris/Wilson,* § 10:14, S. 385.

[527] Vgl. hierzu *Kris/Wilson,* § 28:4, S. 210ff.

[528] Vgl. *Kris/Wilson,* § 9:8.

[529] Vgl. hierzu *Kris/Wilson,* § 28:4, S. 211.

[530] So *Kris/Wilson,* § 28:4, S. 211, die einen Versicherungsbetrug als Beispiel wählen.

[531] Vgl. *United States v. Isa*, 923 F.2d, 1300, 1304 (8th Cir. 1991). Vgl. zu diesem Beispiel *Kris/Wilson,* § 9:8, S. 346.

Verbindung zum geheimdienstlichen Aufklärungsauftrag stand, leitete das FBI die erhobenen Erkenntnisse an die zuständigen Strafverfolgungsbehörden weiter. Dieses Vorgehen wurde von dem Gericht für zulässig erachtet.

Die *minimization procedures* stehen einer Übermittlung von strafrechtlich relevanten Erkenntnissen letztlich nicht im Wege. Entweder werden sie ausdrücklich gestattet oder sie fallen als *foreign intelligence crimes* von vorneherein nicht in den Anwendungsbereich der Verfahrensregeln. Etwas anderes gilt nur bei Überwachungsmaßnahmen, die ausschließlich auf einer Anordnung des *Attorney General* beruhen und damit ohne Anordnung des FISC durchgeführt wurden.[532] Derartige Überwachungsmaßnahmen sind in Konstellationen vorgesehen, die aller Voraussicht nach keine *U.S. Persons* betreffen. Fallen entgegen dieser Vorgabe während der Überwachung dennoch Erkenntnisse über eine *U.S. Person* an, ist deren Weitergabe ausdrücklich verboten. Von diesem Verbot kann nur bei einer Genehmigung des FISC abgesehen werden.[533] Abseits dieser Sonderkonstellation begrenzt das in den *minimization procedures* statuierte Weitergabeverbot eine Übermittlung zu Strafverfolgungszwecken nur in Ausnahmefällen.[534]

(2) Sonstige Voraussetzungen

Neben der Einhaltung der *minimization procedures* wird die Übermittlung von FISA-Erkenntnissen an drei weitere Bedingungen geknüpft. Die zweite Voraussetzung ist die Bindung an einen rechtmäßigen Zweck. Diese Voraussetzung ist auf sämtliche Erhebungsmaßnahmen sowie auf *U.S.* wie *Non-U.S. Persons* und soll eine Heranziehung von FISA-Erkenntnissen zu illegalen Zwecken ausschließen.[535] Die in Bezug auf die Rechtmäßigkeit einer Zwecksetzung bestehenden Unsicherheiten sind vorliegend nicht von Interesse, da zumindest die Nutzung zur Strafverfolgung als legitimer Zweck anerkannt ist.[536] Für die Verfolgung von *foreign intelligence crimes* ergibt sich die Rechtmäßigkeit des Zwecks indirekt aus dem Beitrag zur nationalen Sicherheit. Für sonstige Straftaten kann diese aus der gesetzlichen Anordnung in den Vorschriften des 50 U.S.C. §§ 1801(h)(3), 1821(4)(C), 1861(g)(2)(C) gefolgert werden.

Als dritte Voraussetzung ist die vorherige Beteiligung und Erlaubnis des *Attorney General* erforderlich.[537] Dessen Einschaltung soll eine zentrale Kontrolle

---

[532] Vgl. hierzu *Kris/Wilson,* § 9:10.

[533] Vgl. 50 U.S.C. §§ 1801(h)(4), 1821(4)(D).

[534] Vgl. *Kris/Wilson,* § 28: 2, S. 209.

[535] Vgl. *Kris/Wilson,* § 28:3, S. 209ff.

[536] Vgl. *Kris/Wilson,* § 28:4, S. 209ff.

[537] 50 U.S.C. § 1806(b) *(electronic surveillance)*, § 1825(c) *(physical search)*, § 1845(b) *(pen/trap)*, vgl. auch *Kris/Wilson,* § 28:4, S. 213f.

sicherstellen, sodass dieses Erfordernis sowohl bei einer Übermittlung an Staatsanwaltschaften des Bundes als auch der Einzelstaaten zur Anwendung kommt.[538]

Als vierte Voraussetzung muss die Übermittlung unter Aufrechterhaltung bestehender Privilegien erfolgen.[539] Derartige Privilegien können beispielsweise bei einem Austausch vertraulicher Informationen zwischen Ehegatten oder dem Verteidiger mit seinem Mandanten entstehen.[540] Durch die gesetzliche Vorgabe soll sichergestellt werden, dass die privilegierte Kommunikation ihren Status nicht durch die Abhörmaßnahmen Dritter verliert.[541] Die Regelung des FISA hat insofern lediglich klarstellenden Charakter.[542] Die Reichweite und der Umfang der Privilegien werden durch den FISA nicht berührt.

(3) Rechtsfolgen

Sind die genannten Voraussetzungen erfüllt, greift zumindest für Ermittlungen des FBI auf der Grundlage des FISA die in den Mukasey Guidelines angeordnete Übermittlungspflicht.

Als zweite Konsequenz ist die Übermittlung mit einer Mitteilung an das Gericht und den Betroffenen verbunden.[543] Hierbei handelt es sich um eine absolute Ausnahmeregelung des FISA, der anders als strafrechtliche Ermittlungen selbst nach Abschluss der Ermittlungen keine Offenlegung durch Mitteilung, sondern im Grundsatz eine strikte Geheimhaltung vorsieht.[544] Für das Entstehen der Mitteilungspflicht muss die Regierung daher beabsichtigen die Erkenntnisse als Beweismittel gegen eine bestimmte Person zu nutzen.[545] Zudem muss diese Person, deren Eigentum oder Kommunikationsmittel Ziel oder Gegenstand der Überwachungs-

---

538 Vgl. *Kris/Wilson,* § 28:4, S. 215; § 28:5, S. 219.

539 50 U.S.C. § 1806(a) *(electronic surveillance)*; § 1861(h) *(tangible things)* lauten: "No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character." Trotz einer vergleichbaren Gefährdungslage wird dieser Schutz nicht auf Durchsuchungsmaßnahmen erweitert.

540 Für den Erhalt des Privilegs muss zunächst dessen Anwendbarkeit bejaht werden.

541 Grundsätzlich fehlt es an der Vertraulichkeit, wenn Dritte von der Kommunikation Kenntnis nehmen können; vgl. *Kris/Wilson,* § 28:6, S. 220f.

542 Vgl. hierzu *Kris/Wilson,* § 28:6, S. 221.

543 Diese Vorgabe gilt für die Nutzung als Beweismittel in Zivil-, Verwaltungs- und Strafverfahren; vgl. *Kris/Wilson,* § 29:4, S. 230.

544 So *Kris/Wilson,* § 29:1, S. 226. Die Mitteilungspflicht ist allerdings keine Zulässigkeitsvoraussetzung für die Übermittlung, vgl. *Vervaele,* Utrecht L. Rev. (1) 2005, S. 6.

545 Sog. *notification.* Siehe 50 U.S.C. §§ 1806(c) *(electronic surveillance)*, 1825(d) *(physical search)*, 1845(c) *(pen/trap)*. Auf Ebene der Einzelstaaten muss zusätzlich der *Attorney General* benachrichtigt werden. Siehe 50 U.S.C. §§ 1806(d) *(electronic surveillance)*, 1825(e) *(physical search)*, 1845(d) *(pen/trap)*.

maßnahme gewesen sein.[546] Bei einer elektronischen Telekommunikationsüberwachung ist zudem eine Beteiligung an der Kommunikation selbst erforderlich.[547] Daran fehlt es beispielsweise, wenn die Erkenntnisse aus einer Kommunikation von Dritten stammen.[548] Inhaltlich werden regelmäßig nur allgemeine Hinweise mitgeteilt, in denen auf die Durchführung der FISA-Überwachung und auf eine entsprechende Nutzungsabsicht hingewiesen wird.[549] Konkrete Offenlegungsfragen werden demgegenüber erst in der *discovery*-Phase geklärt.[550]

cc) Sonstige Übermittlungspflichten

Außerhalb der geheimdienstlichen Vorschriften können die Dienste aufgrund der strafprozessualen Offenlegungspflichten zu einer Übermittlung verpflichtet sein. Von einer derartigen Konstellation ist beispielsweise auszugehen, wenn die Geheimdienste selbst aktiv die Ermittlungen der Strafverfolgungsbehörden unterstützen oder aktiv daran teilnehmen. Die Gerichte sprechen in diesem Fall von Behörden "closely aligned with the prosecution".[551] In diesem Fall gelten die Offenlegungspflichten nicht nur für die Staatsanwaltschaft, sondern zusätzlich für sämtliche Behörden, die mit ihr zusammenarbeiten.[552] Bei einer Kooperation mit dem Geheimdienstsektor erstrecken sich die Offenlegungspflichten damit zugleich auf die Unterlagen der involvierten Geheimdienste.[553] Derart aktive Ermittlungsbeiträge sind vor allem im Bereich der Terrorbekämpfung und des internationalen Drogenhandels denkbar und können zu einer Übermittlungspflicht der Dienste führen.[554]

b) Übermittlung auf Anfrage

Neben der eigenständigen Übermittlung kann die Informationsweitergabe auf einer entsprechenden Anfrage an die Dienste beruhen. Für die Anfrageübermittlung

---

[546] 50 U.S.C. § 1801(k). Die bloße Namensnennung genügt nicht, vgl. *Kris/Wilson,* § 29:5, S. 293. Ebenso 50 U.S.C. § 1821(2) *(physical search)*, § 1841(3)(A), (B) *(pen/trap)*.

[547] 50 U.S.C. §§ 1806(c) spricht von „information obtained or derived from an electronic surveillance of that aggrieved person".

[548] Vgl. *Kris/Wilson,* § 29:5, S. 235.

[549] Insgesamt vertiefend *Kris/Wilson,* § 29:11, S. 242f.

[550] Vgl. *Kris/Wilson,* § 29:11, S. 242f.

[551] Siehe *United States v. Brooks*, 966 F.2d 1500, 1503 (D.C. Cir. 1992).

[552] Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 347; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 422f. Vgl. zu dieser Tendenz *Baker,* Foreign Policy (97) Winter 1994–1995, S. 45.

[553] Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 347f.

[554] Vgl. *Kris/Wilson,* § 2:14; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 422f.

gelten die Voraussetzungen, die bereits bei der eigenständigen Übermittlung der Geheimdienste dargestellt wurden.

c) Zwischenergebnis zu Übermittlungsregeln

Die Übermittlung von Geheimdienstinformationen zu Zwecken der Strafverfolgung wird umfassend gestattet. Selbst die Übermittlung von FISA-Erkenntnissen unterliegt keinen nennenswerten inhaltlichen Beschränkungen. Es werden weder bestimmte Übermittlungsschwellen noch das Vorliegen schwerer Delikte gefordert. Lediglich in Bezug auf Informationen zu *U.S. Persons* finden sich vereinzelte Regelungen.

4. Verwertung von Geheimdienstinformationen

Die Verwertung geheimdienstlicher Erkenntnisse ist im amerikanischen Recht im Grundsatz ebenso unproblematisch wie deren Übermittlung. Demnach dürfen zunächst alle unter Beachtung der Erhebungsvorschriften gesammelten und nach den Mukasey Guidelines beziehungsweise FISA-Regeln übermittelten Erkenntnisse nach den allgemeinen Beweisregeln verwertet werden.[555] Diese klassischen Verwertungsgrundsätze können bei einer Nutzung von Geheimdienstinformationen allerdings zu erheblichen Einschränkungen führen. Die nachfolgende Darstellung widmet sich daher den allgemeinen Herausforderungen einer Verwertung von Geheimdienstinformationen (a), den spezialgesetzlichen Vorgaben des FISA (b) sowie der beweisrechtlichen Berücksichtigung möglicher Fehlerquellen im geheimdienstlichen Erhebungs- und Übermittlungsprozess (c).

a) Allgemeine Verwendungs- und Verwertungsregeln

Inhaltlich werden an die Verwertung von Geheimdienstinformationen die gleichen Maßstäbe angelegt, die auch bei anderen Beweismitteln gelten.[556] Diese Vorgaben ergeben sich vor allem aus der Verfassung, den FRCrimP und den FRE. Darüber hinaus werden keine zusätzlichen Anforderungen aufgestellt. Aufgrund der besonderen Erhebungsbedingungen des Geheimdienstsektors ist die einschränkende Wirkung dieser Beweisregeln allerdings weitaus größer als bei klassischen

---

[555] Vgl. allgemein *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); *United States v. Ning Wen*, 477 F.3d 896, 897ff (7th Cir. 2007); *Arzt,* in: Graulich/Simon, S. 260; *Bradley,* Tul. L. Rev. (77) 2002, S. 484; *Gurulé/Corn,* S. 228; *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 151, 153; *McNamara,* in: Markle Foundation, S. 90; *Standler*, S. 11, 37; *Zabel/Benjamin,* S. 77.

[556] Vgl. *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 422f.

Beweismitteln.[557] Die mit einer beweisrechtlichen Nutzung von Geheimdienstinformationen verbundenen Herausforderungen liegen insofern weniger im rechtlichen als vielmehr im tatsächlichen Bereich. So kann etwa auf die Einhaltung bestimmter Vorgaben verzichtet werden, wenn perspektivisch kein Strafverfahren angestrebt wird.[558] Dies ist bei geheimdienstlichen Ermittlungen vor allem dann der Fall, wenn sich sonst die Chancen einer geheimdienstlichen Aufklärung oder militärischen Operation verschlechtern würden.[559] Werden die geheimdienstlichen Erkenntnisse entgegen der ursprünglichen Intention dennoch einer beweisrechtlichen Nutzung zugeführt, können die klassischen Beweisregeln einer Verwertung als Beweismittel entgegenstehen. Die damit verbundenen Schwierigkeiten und Besonderheiten werden nachfolgend am Beispiel der *hearsay rule* und der *Miranda warnings* vertieft.

Nach der sogenannten *Miranda*-Entscheidung können Geständnisse aus einer haftbedingten Vernehmungssituation nur verwertet werden, wenn der Verdächtige vorab über seine Rechte belehrt wurde.[560] Voraussetzung einer Belehrungspflicht ist damit ein formaler Festnahmeakt *(custody)* und das Bestehen einer Vernehmungssituation *(interrogation)*.[561] Die als *Miranda warnings* bekannten Belehrungspflichten gelten für sämtliche inländischen Ermittlungen und damit grundsätzlich auch für Maßnahmen der Geheimdienste. Sobald eine Haftsituation vorliegt, sind die Dienste damit ebenfalls zur Beachtung der Belehrungspflichten angehalten.[562] Diese Verlesung der Beschuldigtenrechte ist eine wesentliche Voraussetzung für die Verwertbarkeit.[563] Sehen die Geheimdienste daher aus ermittlungstaktischen Gründen von einer Belehrung ab, können die Erkenntnisse grundsätzlich nicht als Beweismittel herangezogen werden.[564]

Von dieser Grundregel ergeben sich in terrorrelevanten Sachverhaltskonstellationen erhebliche Ausnahmen. Bei Vernehmungssituationen im Ausland gelten die Belehrungspflichten beispielsweise nur, wenn es sich bei dem Vernommenen oder

---

[557] Vgl. *Gitenstein,* in: Wittes, S. 16; *Litt/Bennett,* in: Wittes, S. 152. Vgl. zu einer Diskussion dieser Beweisregeln *Zabel/Benjamin,* S. 107ff.

[558] Vgl. zu dem Verzicht auf den Richtervorbehalt, wenn ein Strafverfahren nicht absehbar ist, *Fenske,* NULR (102) 2008, S. 346; *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 334.

[559] Vgl. *Fenske,* NULR (102) 2008, S. 347, 377, der bei DII für einen Verzicht auf das *warrant*-Erfordernis plädiert und stattdessen eine nachträgliche gerichtliche Prüfung der *reasonableness* bzw. vorherige Einwilligung des *Attorney General* i.S.d. FISA favorisiert.

[560] *Miranda v. Arizona*, 384 U.S. 436 (S. Ct. 1966). Anknüpfungspunkt ist die Selbstbelastungsfreiheit und das Recht auf einen Verteidiger nach dem 5. und 6. Verfassungszusatz.

[561] Vgl. *Rogall,* Theorie, S. 127; *Trüg,* S. 420; *Zabel/Benjamin,* S. 10, 101ff. Vgl. zum Inhalt der Belehrung *Doyle,* CRS 2013, S. 1ff; *Signorelli,* S. 286.

[562] Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 20.

[563] Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 40.

[564] Vgl. *Zabel/Benjamin,* S. 102.

der Vernehmungsperson um eine *U.S. Person* handelt.[565] Selbst im Inland wird die bislang klare Geltung der Belehrungspflichten durch die Ausweitung der sogenannten *public safety exception* teilweise infrage gestellt. Nach der *public safety exception* können in bestimmten Ausnahmefällen Geständnisse verwertet werden, die ohne Belehrung zustande gekommen sind.[566] Die bis dato für akute Gefahrenlagen gedachte Ausnahmeregelung wurde durch eine Richtlinie des *Attorney General* Eric Holder Ende 2010 auf den Bereich des Terrorismus ausgedehnt.[567] In der ursprünglichen Fassung war ein solcher Ausnahmefall nur gegeben, wenn erstens eine akute Gefahr für die öffentliche Sicherheit die Belehrung im Zeitpunkt der Vernehmung unmöglich macht und zweitens die Verlesung unverzüglich nach Auflösung der Gefahrensituation nachgeholt wurde.[568] Diese Voraussetzungen wurden nun Ende 2010 auf die Bedürfnisse der Geheimdienste angepasst. Danach wird die *public safety exception* auf Fälle ausgeweitet, in denen eine unmittelbare Belehrung die Erhebung wertvoller Geheimdienstinformationen gefährden würde. Diese Ausnahme kam beispielsweise im Zusammenhang mit den Anschlägen auf den Boston-Marathon im April 2013 zum Tragen und ermöglichte den Behörden eine zeitlich verzögerte Belehrung des Verdächtigen *Dzhokhar Tsarnaev*.[569]

Allerdings erfordert die *public safety exception* keine unmittelbar bevorstehende Gefahr.[570] Dies lässt vermuten, dass die Verwertung von Geständnissen selbst dann möglich ist, wenn die Belehrung nur aus ermittlungstaktischen Gründen aufgeschoben wurde. Es wird zwar betont, dass die Ausnahme nicht gezielt zur Erhebung von Beweismaterial eingesetzt werden darf, dennoch sind negative Auswirkungen auf die Beschuldigtenrechte nicht von vorneherein auszuschließen.[571] Wahrscheinlicher ist vielmehr, dass durch die Ausweitung der *public safety excep-*

---

[565] Maßgeblich ist nicht der Ort der Aussage, sondern der des Strafverfahrens, da erst dort die Rechtsverletzung erfolgt; vgl. *Zabel/Benjamin,* S. 102. Vertiefend zur Geltung von Miranda-Rechten im Ausland *Doyle,* CRS 2013, S. 5f.

[566] Vgl. *Trüg,* S. 434ff.

[567] Vgl. zur öffentlichen Diskussion Los Angeles Times vom 12. Mai 2010, abrufbar unter http://articles.latimes.com/2010/may/12/opinion/la-ed-miranda-20100513 [Stand: 1.5.2012].

[568] Vgl. *New York v. Quarles* 467 U.S. 649, 655f (1984). Allgemein zur Beachtlichkeit zeitlich verzögerter Belehrungen 18 U.S.C. 3501(c) sowie *Corley v. United States*, 556 U.S. 303, 317 (3d Cir. 2009); vgl. zudem *Rogall,* in: Wolter, S. 128; *Scheb/Scheb II,* S. 352; Stimson 2010, S. 1. Vertiefend zur public safety exception *Doyle,* CRS 2013, S. 3f.

[569] Siehe unter anderem die Beiträge http://abcnews.go.com/blogs/politics/2013/04/next-for-bombing-suspect-high-value-detainee-interrogation-group/; http://www.huffingtonpost.com/2013/04/22/dzhokhar-tsarnaev-miranda_n_3134745.html [Stand: 5.6.13].

[570] So die Beiträge von *Reilly,* TPM vom 24.3.2011; ebenso *Perez,* The Wall Street Journal vom 24.3.2011. Danach sei die Regelung auf Sonderfälle anwendbar in denen die Ermittler "conclude that continued unwarned interrogation is necessary to collect valuable and timely intelligence not related to any immediate threat." Formal genügt die Bewilligung des Dienstvorgesetzten und der Rechtsberater des Justizministeriums.

[571] Vgl. zur Beschränkung *Litt/Bennett,* in: Wittes, S. 161.

tion der Umfang der tatsächlich verwertbaren Geheimdienstinformationen vergrößert wird. Dies ist von umso größerem Interesse als einem Verstoß gegen die Belehrungspflichten ohnehin keine Fernwirkung zukommt.[572]

Die im Zusammenhang mit den Belehrungspflichten geltenden Besonderheiten werden im Zuständigkeitsbereich einer Militärkommission noch weiter ausgebaut. Begründet wird dies mit den praktischen und taktischen Bedürfnissen einer Kampfsituation, in welcher die Soldaten nicht in gleicher Weise auf eine wirksame Verlesung der Beschuldigtenrechte hinwirken könnten.[573] Die insofern gelockerten Standards setzen sich auf Ebene der Beweisverwertung fort. Danach kann eine Aussage vor einer Militärkommission selbst ohne formale Belehrung verwertet werden, solange die Aussage selbst freiwillig war.[574] Es ist damit ein noch umfassenderer Verzicht auf die Belehrungspflichten möglich. Die an die Verwertung von Geständnissen angelegten Standards sind im Vergleich zur klassischen Strafgerichtsbarkeit aber auch insgesamt deutlich abgesenkt. Dies wird unter anderem daran deutlich, dass unter Folter erlangte Aussagen zwar einem Beweisausschluss unterliegen, diese jedoch mittelbar verwertet werden dürfen.[575]

Eine zweite Herausforderung ergibt sich aus der *hearsay rule* und der insofern geringeren Verwertbarkeit mittelbarer Beweise. Dieser Unterschied spielt bei der Verwertung von Geheimdienstinformationen vor allem aufgrund der besonderen Erhebungsbedingungen eine zentrale Rolle. Anders als klassische Maßnahmen der Beweiserhebung fokussieren die Dienste nicht punktuell ein konkretes Delikt, sondern nehmen einen strategischen und langfristigen Beobachtungsauftrag wahr. Ziel ist eine möglichst umfassende Aufklärung, nicht die Erlangung unmittelbarer Beweismittel. Vielmehr werden beim Fehlen anderweitiger Erkenntnisquellen zusätzlich mittelbar gewonnene Informationen erfasst.[576] Deren Verwertung steht oftmals im Widerspruch zu den Vorgaben der *hearsay rule* in den FRE *Rule* 802–804 beziehungsweise des *Confrontation Clause* des sechsten Verfassungszusatzes und kann damit die beweisrechtliche Nutzung von Geheimdienstinformationen behindern.[577] Da sie jedoch ihrerseits durch zahlreiche Ausnahmen durchbrochen werden, sollte die Wirkung dieser Beweisregeln nicht überschätzt werden.[578] In einem Verfahren vor einer Militärkommission gelten zudem von vorneherein ge-

---

572 So *United States v. Patane*, 542 U.S. 630, 642 (S. Ct. 2004); *Oregon v. Elstad*, 470 U.S. 298, 304 (S. Ct. 1985); vgl. zudem *Doyle,* CRS 2013, S. 2.

573 Vgl. insgesamt *Litt/Bennett,* in: Wittes, S. 161.

574 Vertiefend *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 41.

575 Siehe 10 U.S.C. § 948r(a). Vertiefend *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 41, 42 Fn. 121.

576 Vgl. hierzu *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 46.

577 Vgl. hierzu *Chesney,* in: Commission of Inquiry, S. 91; *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 46; *Thompson/Nored/Worrall/Hemmens,* S. 15.

578 Vgl. hierzu *Zabel/Benjamin,* S. 109f.

lockerte Standards.[579] Nach den dortigen Verfahrensregeln ist die Verwertung von *hearsay evidence* grundsätzlich gestattet, wenn das unmittelbare Beweismittel aus praktischen Gründen nicht verfügbar ist. Eine solche Unverfügbarkeit kann beispielsweise aus dem entfernten Aufenthaltsort des Zeugen oder den besonderen militärischen oder geheimdienstlichen Umständen resultieren.

Die Nutzung von Geheimdienstinformationen unterliegt im Ergebnis den klassischen Beweisregeln des amerikanischen Strafverfahrensrechts. Diese limitieren deren Heranziehung als Beweismittel weit weniger als zunächst erwartet. Die strikten Beweisregeln werden in ihrer Wirkung zunehmend durch allgemeine oder spezielle Ausnahmeregelungen abgeschwächt. Noch geringere Standards gelten im Zuständigkeitsbereich einer Militärkommission, deren Beweisregeln die Verwertung von Geheimdienstinformationen kaum einschränken.

b) Spezialgesetzliche Beschränkungen, insbesondere FISA

Die Verwertung von FISA-Erkenntnissen unterliegt ebenfalls den klassischen Beweisregeln. Die vorgenannten Ausführungen sind damit weitgehend übertragbar. Bemerkenswert ist, dass die umfassende Verwertbarkeit von FISA-Erkenntnissen erst durch die Reformen von 2001 ermöglicht wurde. Vor diesem Zeitpunkt war die strafprozessuale Nutzung an die Einhaltung des sogenannten *primary purpose*-Tests gebunden. Danach waren FISA-Erkenntnisse nur verwertbar, wenn sie aus einer Überwachungsmaßnahme stammten, deren primärer Zweck dem Erhalt von *foreign intelligence* und nicht der Erhebung von Beweismitteln galt.[580] Diese Vorgabe wurde durch die Änderungen des FISA im Jahr 2001 aufgegeben, was die Entscheidungen des FISCR im Jahr 2002 bestätigt wurde. Seitdem gilt der sogenannte *significant purpose*-Standard, wonach die Auslandsaufklärung lediglich einen wesentlichen Zweck der Maßnahme darstellen muss.[581] Eine Verwertung von FISA-Erkenntnissen scheidet nach diesem Standard erst aus, wenn die FISA-Überwachung ausschließlich zur Aufklärung gewöhnlicher Kriminalität durchgeführt wurde und damit von Anfang an jegliche Beziehung zwischen der Überwachung und den nachrichtendienstlichen Aufgaben fehlt.[582] Solange ein Konnex zur Auslandsaufklärung besteht, ist die gleichzeitige Verfolgung strafrechtlicher Zwecke unschädlich.[583]

---

[579] 10 U.S.C. § 949a(b)(3)(D); vgl. zudem *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 46.

[580] Vgl. *Grunwald,* S. 85, sowie insgesamt *A. McCarthy*.

[581] Vgl. 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B); *Becker,* RIDP/IRPL 2009, S. 348; *Grunwald,* S. 88; *Kris/Wilson,* § 10:10, S. 375; *Logan,* N.Y.U. J.L. & Liberty (4) 2009, S. 230. Zur unklaren Reichweite des wesentlichen Zwecks vgl. *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 151.

[582] Vgl. *Arzt,* in: Graulich/Simon, S. 259; *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 152f; *Johnson,* I/S: J.L. & Pol'y for Info. Soc'y (5:3) 2010, S. 423; *Kris/Wilson,* § 10:14, S. 375.

[583] Vgl. hierzu *Johnson,* I/S: J.L. & Pol'y for Info. Soc'y (5:3) 2010, S. 423.

Die im Vergleich zu strafrechtlichen Überwachungsmaßnahmen abweichenden Ermittlungsschwellen und -voraussetzungen des FISA werden beweisrechtlich nicht berücksichtigt. Der Zusammenhang zur auslandsbezogenen Auslandsaufklärung spielt bei der Beweisverwertung dementsprechend keine Rolle, solange die Erkenntnisse selbst rechtmäßig erhoben wurden.[584] Argumentativ kann die Verwertbarkeit unter anderem darauf gestützt werden, dass bei einer rechtmäßigen Überwachung der für eine Ausschlussregelung erforderliche Anknüpfungspunkt fehlt.[585] In einem Urteil von 2006 heißt es unter Bezugnahme auf den FISA: "[T]here is no basis for a district court to reject evidence that was properly gathered."[586]

Diese Überlegungen können durch die sogenannte *plain view exception* ergänzt werden.[587] Diese Ausnahme gestattet eine polizeiliche Beschlagnahme ohne richterliche Anordnung, wenn die fraglichen Gegenstände während einer rechtmäßigen Ermittlungsmaßnahme entdeckt werden. Die Ausnahme greift selbst dann, wenn die Ermittler von vorneherein davon ausgehen, die entsprechenden Gegenstände vorzufinden. Diese Argumentation wird auf FISA-Überwachungen übertragen. Danach dürfen während einer rechtmäßigen FISA-Überwachung auch strafrechtlich relevante Beweismittel erhoben und verwertet werden.[588] Ausreichend ist, dass die Überwachungsmaßnahme selbst gerechtfertigt war. Der *significant purpose*-Standard begrenzt damit primär die Durchführung von FISA-Überwachungen, nicht aber die Verwertung der durch eine FISA-Überwachung erhaltenen Erkenntnisse. Für eine Zulassung und Verwertung von FISA-Erkenntnissen genügt folglich die Einhaltung der bereits besprochenen Erhebungs- und Übermittlungsvorschriften.[589]

c) Berücksichtigung von Fehlern

Neben den klassischen Beweisregeln kann eine Verwertung von Geheimdienstinformationen durch Fehler im Erhebungs- und Übermittlungsprozess behindert werden. Da die Zulassung von geheimdienstlich gewonnenen Beweismitteln anhand der klassischen Vorgaben zu prüfen ist, kann vor allem der Verstoß gegen verfassungsrechtliche Vorgaben zur Unverwertbarkeit führen. Bei einer Nutzung von Geheimdienstinformationen ergeben sich insofern kaum Abweichungen. Die

---

584 Vgl. *In re Sealed Case*, 310 F.3d at 735, 746 (FISCR 2002); *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 153; *Vervaele,* Utrecht L. Rev. (1) 2005, S. 7.

585 Vgl. *United States v. Ning Wen*, 471 F.3d 777, 778 (7th Cir. 2006).

586 Siehe *United States v. Ning Wen*, 471 F.3d 777, 778 (7th Cir. 2006), bestätigt durch *United States v. Ning Wen*, 477 F.3d 896, 897ff (7th Cir. 2007); vgl. zudem *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 154.

587 Zur Übertragbarkeit vgl. *United States v. Ning Wen*, 471 F.3d 777, 778 (7th Cir. 2006), bestätigt durch *United States v. Ning Wen*, 477 F.3d 896, 897ff (7th Cir. 2007). Diese Ausnahmen geht auf *Horton v. California* 496 U.S. 128, 133 (S. Ct. 1990) zurück.

588 Vgl. zur Entscheidung *Standler*, S. 37.

589 Maßgeblich sind die 50 U.S.C. §§ 1806, 1825, 1845; vgl. *Gurulé/Corn,* S. 236.

nachfolgenden Ausführungen geben einen Überblick über spezifische Fehlerquellen im Geheimdienstsektor und deren Auswirkungen auf die Beweisverwertung.

aa) Eingriffe in den Kernbereich privater Lebensgestaltung

Die in der deutschen Rechtsordnung bestehende beweisrechtliche Relevanz von Eingriffen in den Kernbereich bestimmter Freiheitsrechte wird im amerikanischen Recht nicht anerkannt.[590] Ein entsprechender Beweisausschluss wird weder für klassische Ermittlungen noch für geheimdienstliche Beobachtungsmaßnahmen diskutiert. Solange die Ermittlungen und das sich anschließende Strafverfahren formal rechtmäßig durchgeführt wurden, fehlt der für einen Beweisausschluss erforderliche Anknüpfungspunkt.[591]

bb) Rechtswidrige Erhebung

Die Missachtung von Verfahrensregeln kann in bestimmten Fällen zur Bejahung eines Verwertungsverbots herangezogen werden. In Bezug auf geheimdienstliche Beobachtungsmaßnahmen wurde insofern bereits auf den strategischen Verzicht auf bestimmte Beweisstandards verwiesen. Kommt es in einem solchen Fall wider Erwarten zu einem Strafverfahren, kann die Missachtung bestimmter Erhebungsvorschriften zur Rechtswidrigkeit der Erhebungsmaßnahme und schließlich zur Unverwertbarkeit als Beweismittel führen. Die beweisrechtlichen Auswirkungen unterscheiden sich danach, ob gegen verfassungsrechtliche oder einfachgesetzliche Vorgaben verstoßen wurde.

(1) Verfassungsrechtliche Ausschlussregeln

Die Missachtung verfassungsrechtlicher Vorgaben führt im Grundsatz zum Ausschluss der erhobenen Erkenntnisse.[592] Die unter Verstoß gegen eine Verfassungsnorm rechtswidrig erlangten Beweismittel dürfen den Geschworenen eines Strafverfahrens somit nicht vorgelegt werden.[593] Diese Regeln gelten sowohl für die strafrechtliche als auch die geheimdienstliche Informationserhebung und werden vorliegend anhand der Vorgaben des vierten und fünften Verfassungszusatzes erläutert.

Insbesondere die *exclusionary rule* des vierten Verfassungszusatzes bildet im Rahmen der geheimdienstlichen Informationsgewinnung oftmals den für die Annahme eines Verwertungsverbotes zentralen Dreh- und Angelpunkt. Danach ist die

---

590 Vgl. *Ossenberg,* S. 75ff; *Trüg,* S. 451.

591 Vgl. *Ossenberg,* S. 75ff; *Trüg,* S. 450f.

592 Vgl. *Hay,* Rn. 707; *Young,* Fordham L. Rev. (34) 2001, S. 1049.

593 Vgl. hierzu *Ossenberg,* S. 80; *Rogall,* in: Wolter, S. 121.

Durchführung bestimmter Ermittlungsmaßnahmen an das Bestehen eines hinreichenden Grundes i.S.d. *probable cause* sowie die Erlangung einer richterlichen Anordnung im Sinne eines *warrants* gebunden. Die Missachtung dieses Richtervorbehalts führt regelmäßig zur Annahme eines Verwertungsverbots, sofern keine richterlich anerkannte Ausnahme eingreift.[594] Diese Vorgaben sind nicht nur auf polizeiliches Handeln anwendbar, sondern gelten umfassend für alle staatlichen Ermittlungsmaßnahmen.[595] Für den Bereich der *domestic intelligence investigations* (DII) und damit die geheimdienstliche Aufklärung rein inländischer Sachverhalte wurde die Geltung des vierten Verfassungszusatzes in der bereits mehrfach erwähnten *Keith*-Entscheidung höchstrichterlich festgestellt. Erkenntnisse der DII, die ohne einen *warrant* erlangt wurden, können damit nicht verwertet werden. Dies ist im Bereich der auslandsbezogenen Überwachungsmaßnahmen anders. Dort wurde mit dem FISA im Jahr 1978 ein für *foreign intelligence investigations* (FII) geltendes Sonderregime geschaffen, welches Überwachungsmaßnahmen ohne Erhalt eines klassischen *warrants* gestattet.[596] Die Anordnungsbefugnis wurde aufgrund der besonderen Bedürfnisse der auslandsbezogenen Aufklärung von der normalen Gerichtsbarkeit auf den FISC verlagert. Die durch den FISC erlassene FISA-Anordnung wird von der Mehrheit der amerikanischen Gerichte als gleichwertiger Ersatz für einen *warrant* i.S.d. vierten Verfassungszusatzes anerkannt.[597] Im Anwendungsbereich des FISA ist der Verzicht auf eine klassische richterliche Anordnung damit nicht mit einem Verwertungsverbot verbunden.[598]

Ebenfalls von beweisrechtlicher Relevanz ist die Missachtung des fünften Verfassungszusatzes. Dieser Verfassungszusatz verbürgt, dass niemand zu selbstbelastenden Aussagen gezwungen werden darf und bildet seit dem *Miranda*-Entscheid den verfassungsrechtlichen Anknüpfungspunkt für die Belehrungspflichten.[599] Im Grundsatz führt das Unterlassen einer erforderlichen Belehrung zur Unverwertbarkeit der getätigten Aussagen. Dieser Automatismus kann seit der Ausweitung der *public safety exception* nicht nur bei akuten Gefahrensituationen, sondern auch zugunsten der geheimdienstlichen Informationsgewinnung durchbrochen werden.[600] Aufgrund der erheblichen sicherheitspolitischen Relevanz geheimdienstlicher Erkenntnisse führt eine Verletzung von Belehrungspflichten daher nicht mehr zwingend zur Annahme eines Verwertungsverbots.

---

[594] Vgl. zu dieser Diskussion *Weeks v. United States*, 232 US 383, 393 (1914); *Rogall,* in: Wolter, S. 124; *Scheb/Scheb II,* S. 348.

[595] Vgl. *Trüg,* S. 413.

[596] Vgl. zur historischen Entwicklung dieser Ausnahme *Kerr,* Tex. L. Rev. (88) 2010, S. 1676.

[597] Vgl. *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); *United States v. Ning Wen*, 477 F.3d 896, 897ff (7th Cir. 2007).

[598] Vgl. *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005).

[599] Vgl. *Miranda v. Arizona* 384 U.S. 436 (S. Ct. 1966). Vertiefend vgl. *Trüg,* S. 418, 420.

[600] Allgemein zur *public safety exception*, vgl. *Trüg,* S. 436.

Die Missachtung oder Nichtbeachtung verfassungsrechtlicher Vorgaben ist bei einer geheimdienstlichen Informationserhebung damit nicht unbedingt mit einer bedingungslosen Unverwertbarkeit des späteren Beweismittels verbunden. Das ursprünglich starre System der Beweisausschlussregeln wurde im Lauf der Zeit durch verschiedene Ausnahmen durchbrochen.[601] Diese Tendenz wird durch die im amerikanischen Recht bestehende Beweislastverteilung verstärkt. Danach liegt die Beweislast für das Bestehen eines Beweisverwertungsverbots grundsätzlich beim Beschuldigten beziehungsweise Angeklagten.[602] Dieser muss damit je nach Verstoß den Nachweis rechtswidrigen Handelns selbst erbringen. Hierzu wird er aufgrund der umfassenden Geheimhaltung geheimdienstlicher Ermittlungen nicht immer in der Lage sein.

(2) Einfachgesetzliche Ausschlussregeln

Neben der Verletzung von Verfassungsrecht kann die Missachtung einfachgesetzlicher Vorgaben einen Beweisausschluss nach sich ziehen. Voraussetzung ist in diesem Fall das Bestehen eines ausdrücklich gesetzlich normierten oder richterlich herausgebildeten Ausschlussgrundes.[603] Derartige Ausschlussregeln sind regelmäßig strikter als die auf einem Verfassungsverstoß beruhenden *exclusionary rules*. Die Reichweite derartiger Ausschlussregeln wird für den Geheimdienstsektor beispielhaft anhand der Telekommunikationsüberwachung dargestellt. Die bei der geheimdienstlichen Informationsgewinnung diesbezüglich zentralen Ausschließungsgründe richten sich für *domestic intelligence investigations* mangels eigenständiger Ermächtigungsgrundlage nach dem bereits bekannten Title III sowie für *foreign intelligence investigations* nach dem FISA.

In Title III werden die verfassungsrechtlich vorgesehenen Nichtzulassungsgründe erweitert.[604] Nach 18 U.S.C. § 2515 scheidet eine beweisrechtliche Nutzung aus, wenn durch die Offenlegung der Information gegen die Vorgaben des Title III verstoßen werden würde.[605] Da es sich bei dieser Vorschrift nicht um sogenanntes *self-executing law* handelt, kann der Beklagte den Nachweis eines Verstoßes nur auf die in 18 U.S.C. § 2518(10)(a) abschließend genannten Gründe stützen.[606] Eine Nichtzulassung kann demzufolge erstens auf einer rechtswidrigen Durchführung der

---

601 Vgl. *Ossenberg,* S. 80, 88.

602 Vgl. *Rogall,* in: Wolter, S. 136.

603 Vgl. hierzu *Rogall,* in: Wolter, S. 122.

604 Vgl. *Trüg,* S. 409ff.

605 Dort heißt es: "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial […] if the disclosure of that information would be in violation of this chapter."

606 Vgl. *United States v. Philips*, 540 F.2d 319, 325 (8th Cir. 1976); *Boerman,* N.Y.U. J.L. & Liberty (3) 2008, S. 623.

Überwachungsmaßnahme, zweitens auf einer unzureichenden Anordnung sowie drittens auf einem Verstoß gegen die Vorgaben in der Anordnung beruhen.[607] Die Entscheidung selbst steht im Ermessen des Richters.[608] Von einer unzureichenden Anordnung i.S.d. zweiten Variante ist beispielsweise auszugehen, wenn der hinreichende Grund i.S.d. *probable cause* oder die Notwendigkeit einer elektronischen Überwachungsmaßnahme nicht ausreichend dargelegt wurden. Ebenfalls in Betracht kommen eine nicht hinreichend präzisierte Überwachungsanordnung oder eine Missachtung der Anordnungskompetenzen. Ein Verstoß gegen die Anordnung i.S.d. dritten Variante ist bei einer Verletzung der Verhältnismäßigkeitsregeln der *minimization procedures* oder einer fälschlichen Überwachung denkbar, etwa wenn anstelle der mündlichen die drahtgebundene Kommunikation überwacht wurde.[609] Die im Title III normierten Ausschlussgründe sind damit vergleichsweise umfassend. Dies kommt nicht zuletzt darin zum Ausdruck, dass die Anwendbarkeit der *good faith exception* im Rahmen des Title III umstritten ist.[610] Diese Weite der genannten Ausschlussmöglichkeiten wird durch die Rechtsprechung allerdings auf solche Verstöße begrenzt, denen nach dem Willen des Gesetzgebers eine zentrale Rolle zukommt.[611] Dies soll zur Unbeachtlichkeit sogenannter *technical violations* führen, da den speziell gesetzlich angeordneten Ausschlussgründen sonst keine praktische Bedeutung mehr zukäme.[612] Diese Ansicht wird von den Gerichten geteilt, denen zufolge die Vorschriften des Title III eine eigenständige *exclusionary rule* normieren.[613]

Die im Anwendungsbereich des FISA geltenden Ausschlussgründe stimmen mit denen des Title III weitgehend überein.[614] Eine Nichtzulassung kann danach sowohl auf eine rechtswidrige Informationserhebung als auch einen Verstoß gegen

---

[607] Vgl. hierzu 18 U.S.C. § 2518(10)(a): "may move to suppress […] on the grounds that (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval"; vgl. auch *Boerman,* N.Y.U. J.L. & Liberty (3) 2008, S. 628ff.

[608] Vgl. 18 U.S.C. § 2515 der die Formulierung "may" verwendet.

[609] Vgl. *Boerman,* N.Y.U. J.L. & Liberty (3) 2008, S. 625; *Kris/Wilson,* § 32:3, S. 284; § 32:4, S. 286.

[610] Die Anwendbarkeit ist zwischen den verschiedenen Bezirksgerichten umstritten. Der 8. und 11. Bezirk bejahen die Anwendbarkeit, vgl. *United States v. Moore*, 41 F.3d 370, 376 (8th Cir. 1994); *United States v. Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988) während der 6. Bezirk diese ablehnt, vgl. *United States v. Rice*, 478 F.3d 704, 713 (6th Cir. 2007) sowie *Boerman,* N.Y.U. J.L. & Liberty (3) 2008, S. 626.

[611] Vgl. *United States v. Chavez*, 416 U.S. 562, 578 (S. Ct. 1974); *United States v. Giordano*, 416 U.S. 505, 527 (S. Ct. 1974) sowie *Boerman,* N.Y.U. J.L. & Liberty (3) 2008, S. 623; *Kris/Wilson,* § 32:3, S. 284; *Trüg,* S. 409.

[612] Vgl. *Boerman,* N.Y.U. J.L. & Liberty (3) 2008, S. 624.

[613] Vgl. *United States v. Giordano*, 416 U.S. 505, 558 (S. Ct. 1974).

[614] Vgl. *Kris/Wilson,* § 32:3, S. 283.

die Überwachungsanordnung gestützt werden.[615] Nicht erfasst ist demgegenüber der im Title III enthaltene Ausschlussgrund einer unzureichenden Anordnung. FISA-Erkenntnisse können demnach verwertet werden, solange die Durchführung der Überwachungsmaßnahme selbst rechtmäßig war beziehungsweise im Einklang mit der Anordnung stand.[616] Ähnlich wie im Anwendungsbereich des Title III muss es sich bei der verletzten Norm allerdings um eine zentrale Vorschrift des FISA handeln.[617] Obwohl den meisten FISA-Regeln eine solche zentrale Rolle zugesprochen wird, hat bisher kein Gericht die Zulässigkeit von FISA-Erkenntnissen abgelehnt.[618]

cc) Rechtswidrige Übermittlung

Fehler im Übermittlungsprozess werden nur in seltenen Fällen die Grundlage eines Verwertungsverbots bilden. Den Übermittlungsvorgaben der Mukasey Guidelines kommt in diesem Zusammenhang lediglich eine rein interne Wirkung zu, sodass sie für Außenstehende weder Rechte noch Pflichten begründen. Ein Verstoß gegen die internen Richtlinien ist damit zur Begründung eines Verwertungsverbotes ungeeignet. Die Übermittlung von FISA-Erkenntnissen ist demgegenüber aufgrund gesetzlicher Vorschriften an bestimmte Mindestanforderungen gebunden. Bei der Untersuchung dieser Vorgaben konnte allerdings festgestellt werden, dass diese bei einer Übermittlung zu Strafverfolgungszwecken faktisch keine begrenzende Wirkung entfalten. Eine rechtswidrige Übermittlung ist unter diesen Voraussetzungen damit kaum vorstellbar. Dieses Ergebnis wird vom amerikanischen Gesetzgeber nicht zuletzt durch den Aufbau und Ausbau der sogenannten *information sharing environment* bestätigt. Ein Verwertungsverbot infolge einer rechtswidrigen Weitergabe von Geheimdienstinformationen scheidet damit aus.

dd) Fernwirkung

In Bezug auf die Fernwirkungsproblematik gelten bei einer Nutzung geheimdienstlicher Erkenntnisse keine Besonderheiten.

---

615 Vgl. 50 U.S.C. §§ 1806, 1825, 1845. Diese setzen voraus: "(1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval".

616 In den 50 U.S.C. §§ 1806, 1825, 1845 fehlt der in 18 U.S.C. § 2518(10)(ii) enthaltene Zusatz: "the order of authorization or approval under which it was intercepted is insufficient on its face".

617 Vgl. *Kris/Wilson,* § 32:3, S. 284. Dies entspricht der Regelung des Title III.

618 Vgl. *Kris/Wilson,* § 32:3, S. 284 Fn. 15 sowie S. 285.

d) Aktuelle Kritik an den Verwertungsregeln

Die gegen eine Verwertung von Geheimdienstinformationen vorgebrachte Kritik betrifft vor allem die Beeinträchtigung einschlägiger Verfassungsgarantien sowie die Umgehung sonstiger Erhebungsvoraussetzungen.

aa) Umgehung des vierten Verfassungszusatzes

Ein erster Kritikpunkt betrifft die fehlende Gleichwertigkeit der FISA-Anordnung mit dem klassischen *warrant*. Die Bedenken richten sich vor allem gegen den abweichenden *probable cause*-Standard, die geringere Bestimmtheit der FISA-Anordnung, die längere Dauer von FISA-Überwachungen und die nur schwach ausgeprägte Prüfungskompetenz der FISC-Richter.[619] In Bezug auf *Non-U.S. Persons* werden zudem die abgesenkten Erhebungsstandards bemängelt.[620] Die Kritiker betonen, dass es sich bei einer FISA-Anordnung nicht um ein hundertprozentiges Äquivalent zum strafrechtlichen Richtervorbehalt handele. Die durch die Gerichte[621] festgestellte Vereinbarkeit der FISA-Anordnung mit den Vorgaben des vierten Verfassungszusatzes wird als nicht überzeugend empfunden.[622] Zwar würden die Gerichte die unterschiedlichen Anforderungen des FISA ansprechen, sich jedoch letztlich mit der Feststellung begnügen, dass eine FISA-Anordnung den Anforderungen des vierten Verfassungsschutzes „hinreichend nahe" komme. Die insofern angeführte Ähnlichkeit der FISA-Anordnung ist nach Ansicht der Kritiker nicht ausreichend, um eine anschließende Beweisverwertung rechtfertigen zu können.[623] Sie verweisen darauf, dass man sonst den FISA konsequenterweise auch zur Aufklärung einfacher Kriminalität heranziehen dürfen müsste, was jedoch nicht der Fall sei.[624] Um eine zu ausufernde Nutzung des FISA zu verhindern, wird daher die

---

619 Vgl. *Evans,* Loy. U. Chi. L.J. (33) 2002 , S. 974ff; *Gurulé/Corn,* S. 228ff; *A. Meyer*, S. 34f.

620 Vgl. *Kris/Wilson,* § 11:19.

621 Vgl. *United States v. Hammoud*, 381 F.3d. 316, 333 (4th Cir. 2004), zuletzt erneute Anhörung abgelehnt durch *Hammoud v. U.S.*, S.Ct. 2013 WL 1788146, 81 USLW 616 (U.S. Apr 29, 2013). Einzig in *Mayfield v. United States*, 504 F. Supp. 2d 1023, 1036ff (2007), wurde die Verfassungsmäßigkeit des FISA abgelehnt. Diese Entscheidung wurde jedoch durch *Mayfield v. United States*, 588 F.3d 1252 (9th Cir. 2009) und *Mayfield v. United States*, 599 F.3d 964 (9th Cir. 2010) wieder revidiert. Allgemein *Standler*, S. 31, 34.

622 Siehe *In re Sealed Case,* 310 F. 3d. 717, 746 (FISCR 2002): "we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close". Vgl. *Gurulé/Corn,* S. 230ff.

623 Vgl. *Standler* 2007, S. 36. Dieser vergleicht den Wertgehalt der FISCR-Entscheidung mit einer ärztlichen Aussage wie "If she's not pregnant, she is certainly close to pregnant".

624 So *Hall,* Wake Forest L. Rev. (41) 2006, S. 92.

Einführung einer nachträglichen Nutzungsbeschränkung vorgeschlagen.[625] Diese würde im Gegensatz zu dem *ex ante* ansetzenden *primary purpose*-Test erst im Anschluss an die Informationserhebung greifen, ohne dabei zugleich die Aufklärungsmöglichkeiten in nationalen Sicherheitsfragen zu behindern.

bb) Umgehung des ersten Verfassungszusatzes

Als zweiter Kritikpunkt wird eine unzulässige Beeinträchtigung des ersten Verfassungszusatzes angeführt. Unter dem Stichwort des sogenannten *religious profiling* werden vor allem Bedenken in Bezug auf die Gefahrerforschungsmaßnahmen nach den Mukasey Guidelines geäußert. Da diese eine Überwachung unabhängig von einer Tatsachengrundlage ermöglichen, bestände die Gefahr, dass Beobachtungsmaßnahmen primär auf die Zugehörigkeit zu einer politischen oder religiösen Gruppe gestützt würden.[626] Zwar dürften Überwachungen nicht ausschließlich auf religiösen, ethnischen oder politischen Gründen basieren, dessen ungeachtet würden derartige Aspekte in der Praxis zumindest ergänzend mit einbezogen.[627] Die bewusste beziehungsweise unbewusste Berücksichtigung dieser Merkmale werde durch die Unbestimmtheit der aktuellen Richtlinien begünstigt. Der im Grundsatz vollumfängliche Schutz des ersten Verfassungszusatzes könne bei geheimdienstlichen Ermittlungen damit relativ leicht umgangen werden.[628] Es bestehe daher die Gefahr, dass Betroffene von der Wahrnehmung ihrer religiösen und persönlichen Freiheiten abgeschreckt würden.[629]

Diese Abschreckungstendenzen werden nach Ansicht der Kritiker durch eine relativ strenge Rechtsprechungspraxis begünstigt. Danach seien die Gerichte selbst bei einer Verletzung des ersten Verfassungszusatzes sehr zögerlich das für den Beweisausschluss erforderliche *standing* des Klägers zu bejahen. Als Beispiel wird das bereits erwähnte *NSA-Surveillance Program* herangezogen. Dieses gestattete die Überwachung des Telefon- und E-Mail-Verkehrs ohne vorherige richterliche Anordnung, wenn sich einer der Teilnehmer außerhalb der USA befand.[630] Journalisten rügten diese Überwachungstechnik als Angriff auf ihre Pressefreiheit, da ausländische Gesprächspartner aufgrund der drohenden Überwachung von einer Kommunikation abgeschreckt würden.[631] Das Gericht erachtete die bloß subjektiv

---

[625] Vgl. hierzu *Hall,* Wake Forest L. Rev. (41) 2006, S. 63, etwa durch Ergänzung der *minimization procedures*.

[626] Vgl. *Berman*, S. 30; *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 165, 169.

[627] Vgl. *Johnson,* I/S: J.L. & Pol'y for Info. Soc'y (5:3) 2010, S. 444.

[628] So *Berman*, S. 28, bereits unter Bezug auf die Ashcroft Guidelines.

[629] Vgl. mit Beispielen bei *Berman*, S. 28f.

[630] Vgl. *Gurulé/Corn,* S. 224.

[631] Mit diesen verfassungsrechtlichen Bedenken setzt sich *ACLU v. NSA*, 493 F.3d 644, 659 (6th Cir. 2007) auseinander.

empfundene Abschreckung indes als nicht ausreichend.[632] Erforderlich seien vielmehr hinreichend begründete und konkrete Behinderungen.

cc) Umgehung von Erhebungs- und Beweisstandards

Ein weiterer Kritikpunkt betrifft die bei einer strafrechtlichen Nutzung von FISA-Erkenntnissen drohende Verwässerung klassischer Erhebungs- und Beweisstandards. Als Beispiel ist unter anderem die jüngste Ausweitung der *public safety exception* anzuführen, welche einen Aufschub klassischer Belehrungspflichten ermöglicht.[633]

Ebenfalls in der Kritik sind die im Anwendungsbereich der Mukasey Guidelines unpräzisen Ermittlungsstandards.[634] Insbesondere die Maßnahmen der *threat assessment* oder der *preliminary investigations* ließen die Festlegung objektiver Ermittlungsschwellen und -methoden vermissen.[635] Der in den Mukasey Guidelines unter Punkt II.B.4.a.iii. gestattete Einsatz von "all lawful methods" gäbe den Ermittlungsbeamten keine klaren Leitlinien an die Hand. Diese weitläufigen Ermächtigungen könnten den missbräuchlichen Einsatz geheimdienstlicher Methoden kaum verhindern.[636] Schließlich sei durch die Nutzung des FISA eine Umgehung klassischer *minimization procedures* zu befürchten. Während im Anwendungsbereich des Title III alle aufgezeichneten Kommunikationsinhalte umfassend gespeichert und versiegelt würden, seien nach dem FISA alle nicht relevanten und damit unter Umständen sogar entlastenden Erkenntnisse zu löschen. Da die Regierung die Speicherung entlastenden Beweismaterials nicht gewährleisten könne, bestehe bei einer beweisrechtlichen Nutzung von FISA-Erkenntnissen die erhöhte Gefahr einer unvollständigen Sachverhaltsdarstellung.[637] Der von strafrechtlichen Ermittlungen abweichende Selektionsprozess sei in einem späteren Strafverfahren nicht mehr behebbar.

e) Zwischenergebnis zu Verwertungsregeln

Im amerikanischen Kontext ist die Verwertung von Geheimdienstinformationen als problemlos möglich. Insbesondere im Bereich der inlandsbezogenen Aufklärung müssen aufgrund der identischen Erhebungsstandards keine beweisrechtlichen Sonderregeln beachtet werden. Die bei geheimdienstlichen Erkenntnissen grundsätzlich zu erwartende einschränkende Wirkung der klassischen Beweisregeln wird durch

---

632 Vgl. zu diesem Urteil *Gurulé/Corn,* S. 223ff.

633 Eine exakte Einschätzung dieser Neuregelung ist aufgrund der Geheimhaltung der Richtlinie bislang nicht möglich.

634 Vgl. *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 171.

635 Vgl. auch *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 171.

636 So *Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 174.

637 Vgl. *Kris/Wilson,* § 9:6.

verschiedene Ausnahmeregelungen zunehmend aufgeweicht. Darüber hinaus können Erkenntnisse der auslandsbezogenen Aufklärung seit den Reformen von 2001 in den meisten Fällen ebenfalls unabhängig von der ursprünglichen Zielsetzung verwertet werden. Selbst Fehler im geheimdienstlichen Erhebungs- und Übermittlungsprozess sind bei der Beweisverwertung lediglich im Falle eines Verfassungsverstoßes oder bei Vorliegen eines spezialgesetzlichen Ausschlussgrundes von Relevanz. Im Geltungsbereich des FISA sind solche Fehler aufgrund der besonderen Ausgestaltung des Beweiszulassungsverfahrens zudem nur selten nachweisbar.

IV. Auswirkungen staatlicher Geheimhaltung

Der zweite Problemkreis der vorliegenden Untersuchung betrifft die Auswirkungen nationaler Sicherheitsinteressen auf die Nutzungs- und Offenlegungsmöglichkeiten von Geheimdienstinformationen. Die nachfolgenden Ausführungen geben zunächst einen Überblick über die bei einer staatlichen Geheimhaltung bestehenden Interessens- und Rechtskonflikte (A). Im Anschluss werden die in Geheimhaltungsfragen relevanten Vorgaben der E.O. 13526, des *Classified Information Procedures Act* (CIPA) und des FISA diskutiert (B.).

A. Interessen- und Rechtskonflikte bei staatlicher Geheimhaltung

Bei einer strafprozessualen Nutzung von Geheimdienstinformationen kommt es naturgemäß zu einem Konflikt zwischen den staatlichen Geheimhaltungsinteressen und den im Strafverfahrensrecht bestehenden Offenlegungsansprüchen.

1. Geheimhaltungsinteressen des Staates

Von staatlicher Seite besteht ein erhebliches Interesse an der Geheimhaltung sicherheitsrelevanter Erkenntnisse, Methoden und Quellen.[638] Insbesondere für verdeckte Ermittlungen sind die künftige Einsetzbarkeit und der persönliche Schutz des Ermittlers von entscheidender Bedeutung.[639] Zuletzt betonte der *Supreme Court* in einer Entscheidung von 2008 das Geheimhaltungsinteresse der Regierung: "has a legitimate interest in protecting sources and methods of intelligence gathe-

[638] Vertiefend *Chesney,* in: Commission of Inquiry, S. 107; *Holzer,* Fordham L. Rev. 2005, S. 1963; *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. Appendix 1.

[639] Vgl. *United States v. Whitney*, 633 F.2d 902, 911 (9th Cir. 1980) sowie *Thaman,* in: Perron, S. 526. Diese Grundsätze gelten auch für Ermittler der Geheimdienste.

ring".[640] Dieses hat sich im amerikanischen Recht vereinzelt zu anerkannten Privilegien verdichtet. Im Strafverfahren werden Informanten beispielsweise über das *informer's privilege*, nationale Sicherheitsinteressen über das *government privilege* beziehungsweise *classified information privilege* geschützt.[641] In Zivilverfahren existiert zudem das *state secrets privilege.*[642]

2. Offenlegungspflichten und Teilhaberechte

Der staatlichen Geheimhaltung stehen verschiedene Prozessgrundsätze und Teilhaberechte entgegen. Von zentraler Bedeutung sind vor allem die Garantien des fünften und sechsten Zusatzartikels der Bundesverfassung.[643] Der fünfte Verfassungszusatz gewährt unter anderem den Anspruch auf ein rechtsstaatliches und faires Gerichtsverfahren. Danach müssen dem Beschuldigten die effektive Wahrnehmung seiner Verteidigungsrechte und der Zugang zu entlastendem Beweismaterial möglich sein.[644] Der sechste Verfassungszusatz verbürgt mit dem Recht auf einen öffentlichen Prozess, auf Durchführung eines Kreuzverhörs von Belastungszeugen und der Vorladung von Entlastungszeugen ebenfalls in Geheimhaltungsfragen relevante Garantien.[645]

Diese Verfassungsgrundsätze werden durch weitere Offenlegungs- beziehungsweise Akteneinsichtsansprüche der FRCrimP, des *United States Codes* und der Rechtsprechung ergänzt.[646] Diese sogenannten *discovery rights* sollen ein faires Verfahren gewährleisten und die vergleichsweise geringen Ermittlungsressourcen der Verteidigung ausgleichen.[647] Vorliegend sind vor allem die *Brady Rule*, die *Rule* 16 FRCrimP sowie die Regelung des *Jencks Act* in 18 U.S.C. § 3500 von Inte-

---

[640] Vgl. *Boumediene v. Bush*, 553 U.S. 723, 796 (S. Ct. 2008). Ebenso *CIA v. Sims*, 471 U.S. 159, 175 (S. Ct. 1985) – "has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service". Vertiefend *Waxman/Barak-Erez,* Colum. J. Transnat'l L. (48:3) 2009, S. 5.

[641] Vertiefend *Kris/Wilson,* § 26:8, S. 167; *Stacy,* U. Colo. L. Rev. (58) 1987, S. 177; *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1073 Fn. 48.

[642] Zum Teil wird dieses Privileg auch im Rahmen des Strafverfahrens herangezogen. Vgl. zur Diskussion *Donohue,* U. Pa. L. Rev. (159) 2010, S. 210, 215; *Kris/Wilson,* § 26:8, S. 164.

[643] Vertiefend *Scheb/Scheb II,* S. 362; *Turner/Schulhofer,* S. 10ff. Zum persönlichen Anwendungsbereich vgl. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (S. Ct. 1990); *Arzt,* in: Graulich/Simon, S. 246.

[644] Hierbei handelt es sich um den *confrontation clause* und den *compulsory process clause; vgl.* insgesamt *Chesney,* in: Commission of Inquiry, S. 107; *Maggs*, S. 48.

[645] Vgl. *Chesney,* in: Commission of Inquiry, S. 107; *Shea,* Am. Crim. L. Rev. (27) 1990, S. 677, 680; *Thaman,* in: Perron, S. 518; *Turner/Schulhofer,* S. 13.

[646] Vgl. zu den sog. *discovery rights Kris/Wilson,* § 2:14.

[647] *Feeney/Herrmann,* S. 377; *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 339; *Zabel/Benjamin,* S. 110. Auf Ebene der Einzelstaaten finden sich weitgehend Entsprechungen.

resse. Die *Brady Rule* wurde in der Entscheidung *Brady v. Maryland* entwickelt.[648] Sie verpflichtet die Staatsanwaltschaft zur Aufbewahrung und Offenlegung von entlastenden beziehungsweise strafmildernden Beweisen im Besitz der Regierung, sofern diese den Ausgang des Strafverfahrens beeinflussen können.[649] Die Offenlegung muss zu einem Zeitpunkt erfolgen, in dem der Beschuldigte die Erkenntnisse noch zu seinen Gunsten nutzen kann.[650] Die *Rule* 16(a)(1)(E) FRCrimP gilt anders als die *Brady Rule* nicht nur für entlastendes Beweismaterial.[651] Sie gewährt dem Beschuldigten im *pretrial*-Stadium einen Anspruch auf Offenlegung und Herausgabe von Akten, die sich im Regierungsbesitz befinden.[652] Herausgabepflichtig sind sämtliche Urkunden, Augenscheinsobjekte und Sachverständigengutachten. Ausgenommen sind lediglich interne Akten, Protokolle der *grand jury* und der staatsanwaltschaftlichen Zeugenvernehmung.[653] Bei Geltendmachung der Akteneinsicht ist der Beschuldigte seinerseits zur Offenlegung vergleichbarer Unterlagen verpflichtet.[654] Die ebenfalls erwähnte Regelung des *Jencks Act* deckt schließlich den von der *Rule* 16 FRCrimP ausgesparten Bereich der Zeugenaussagen ab. Nach 18 U.S.C. § 3500 muss die Staatsanwaltschaft dem Angeklagten Einsicht in Vernehmungsprotokolle gewähren.[655] Dieses Einsichtsrecht besteht erst, nachdem der Zeuge von der Staatsanwaltschaft in der Hauptverhandlung vernommen wurde.[656] Zudem müssen sich die Protokolle im Regierungsbesitz befinden und sich konkret auf die Zeugenaussage beziehen.[657]

Zwischen den staatlichen Strafverfolgungs- und Geheimhaltungsinteressen einerseits und den Offenlegungs- und Verteidigungsinteressen des Angeklagten andererseits besteht ein erhebliches Spannungsverhältnis, welches durch eine Abwägung der verschiedenen Interessen aufzulösen ist.[658] Das amerikanische Recht

---

[648] In *Brady v. Maryland*, 373 U.S. 83, 87 (1963) heißt es: "We now hold that the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment."

[649] Vertiefend *Feeney/Herrmann,* S. 377; *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 340ff, 345f; *Kris/Wilson,* § 2:14, S. 73; *Maggs*, S. 49; *Thaman,* in: Perron, S. 524; *Trüg,* S. 340. Die Beweislast für die Wesentlichkeit trägt der Beschuldigte.

[650] Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 345f.

[651] Vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 345f.

[652] Vgl. *Kris/Wilson,* § 26:2, S. 134; *Maggs*, S. 48.

[653] Rule 16(a)(2) FRCrimP, vgl. zudem *Trüg,* S. 49.

[654] Rule 16(b)(1)(B) FRCrimP, vgl. zudem *Trüg,* S. 331.

[655] Sog. *statements*; vgl. *Trüg,* S. 332; *Zabel/Benjamin,* S. 110.

[656] Siehe 18 U.S.C. § 3500(a); vgl. *Kris/Wilson,* § 2:14, S. 72f.

[657] Sog. *testimony*; vgl. hierzu *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 342.

[658] Siehe *United States v. Whitney*, 633 F.2d 902, 911 (9th Cir. 1980): "while recognizing the government's legitimate interest in protecting the confidentiality of an informant […] nonetheless requires a balancing of the public interest […] against the individual's right to prepare his defense". Vertiefend *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1066.

stellt die Exekutive dabei grundsätzlich vor die Wahl:[659] Entweder kann sie durch eine Offenlegung die Strafverfolgung ermöglichen und eine Gefährdung nationaler Sicherheitsinteressen in Kauf nehmen oder sie kann sich für eine Geheimhaltung entscheiden, wenn sie im Gegenzug das Strafverfahren ganz oder zum Teil einstellt. Dieses sogenannte *disclose or dismiss*-Dilemma hat der Gesetzgeber erkannt und einer Regelung zuzuführen versucht.[660] Die Grundlagen dieser Geheimhaltungsregeln werden nachfolgend besprochen.

B. Rechtliche Möglichkeiten der Geheimhaltung

Der Umgang mit geheimhaltungsbedürftigen Informationen wird maßgeblich durch den *Classified Information Procedures Act* in *Title 18* U.S.C. Appendix (Abk. CIPA) und dem bereits bekannten FISA geregelt.[661] Beide Vorschriften decken jeweils unterschiedliche Bereiche ab. Die Vorschriften des FISA greifen bei Erkenntnissen, die auf der Grundlage des FISA erhoben wurden und limitieren die Offenlegung der der Überwachung zugrunde liegenden Vorgänge. Die Verfahrensregeln des CIPA kommen dagegen allgemein bei der Nutzung von sogenannter *classified information* zur Anwendung. Dabei handelt es sich um Informationen, die auf der Grundlage spezieller *Executive Orders* als geheimhaltungsbedürftig eingestuft wurden.[662] Der CIPA kennt insofern drei Anwendungsfälle: Erstens, wenn der Angeklagte die Offenlegung von geheimhaltungsbedürftigem Beweismaterial im Regierungsbesitz begehrt, zweitens, wenn der Angeklagte bereits über die Informationen verfügt und im Falle eines Strafverfahrens mit deren Offenlegung droht oder drittens, wenn die Regierung selbst die Nutzung der geheimhaltungsbedürftigen Erkenntnisse beabsichtigt.[663] In aller Regel werden hierzu in einer *pretrial conference* der Ablauf des CIPA-Verfahrens, der Zeitpunkt der *discovery hearings* und die den Parteien obliegenden Offenlegungspflichten festgelegt.[664]

---

[659] Vgl. zu den nachfolgenden Ausführungen *Maggs*, S. 50, 57.

[660] Vgl. *Donohue,* U. Pa. L. Rev. (159) 2010, S. 207.

[661] Im Anwendungsbereich einer Militärkommission gelten mit den 10 U.S.C. § 949p-1 bis § 949p-7 Vorschriften die stark an den CIPA angelehnt sind. Die Parallelität wird in 10 U.S.C. § 949p-1(d) deutlich, wonach sich die Militärrichter primär an der CIPA-Auslegung orientieren sollen, vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 49. Die Darstellung konzentriert sich daher auf die zivile Strafgerichtsbarkeit.

[662] Der Begriff der *classified information* wird in 18 U.S.C. app. § 1 definiert.

[663] Zur Anwendbarkeit auf *classified information* siehe 18 U.S.C. app. § 1. Zum CIPA als Ausdruck eines *classified information privilege* vgl. *Kris/Wilson,* § 26:8, S. 168f.

[664] 18 U.S.C. app. § 2. Wer genau an diesem Verfahrensabschnitt teilhaben darf, ist im CIPA nicht festgelegt. Die Möglichkeit eines *ex parte*-Verfahrens wird allerdings anerkannt, vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 48 Fn. 139. Bei Militärkommissionen ist ein solcher Ausschluss in 10 U.S.C. § 949p-2(b) sogar ausdrücklich vorgesehen. In diesem Verfahrensabschnitt werden nur formale Fragen geklärt.

Parallel zum deutschen Landesbericht werden die einzelnen Geheimhaltungsregeln anhand der unterschiedlichen Geheimhaltungsstrategien untersucht. Für das dem Hauptverfahren vorgelagerte Verfahrensstadium wird auf die *pretrial discovery* abgestellt.[665]

1. Strategie der vollständigen Abschottung

Der Schutz geheimhaltungsbedürftiger Informationen kann durch eine vollständige Abschottung der fraglichen Erkenntnisse erfolgen.

a) Vor der Hauptverhandlung

Vor der eigentlichen Hauptverhandlung kann eine vollständige Abschottung der Informationen auf einer Geheimhaltungsentscheidung der Nachrichtendienste oder einer umfassenden *classification* beruhen.

aa) Geheimhaltungsentscheidung der Nachrichtendienste

Eine vollständige Abschottung des Geheimdienstsektors wird vor allem in Bezug auf FISA-Erkenntnisse akzeptiert.

(1) Voraussetzungen der Geheimhaltung

Die gesetzliche Konzeption des FISA ist bereits von vorneherein auf eine umfassende Geheimhaltung angelegt. Eine Mitteilung an den Betroffenen ist im Regelfall nicht erforderlich.[666] Eine Ausnahme von dieser grundsätzlichen Geheimhaltung kommt nur in Betracht, wenn die Regierung die Erkenntnisse in einem Strafverfahren zulasten des Betroffenen nutzen möchte. Verzichtet die Regierung trotz Vorliegen belastender Erkenntnisse auf deren beweisrechtliche Nutzung, ist sie weder zu einer Mitteilung an den Betroffenen noch zu einer Offenlegung insgesamt verpflichtet. Die als Ermessensvorschriften ausgestalteten Übermittlungs- und Offenlegungsregeln des FISA gestatten insofern eine Abwägung zwischen den für eine Offenlegung sprechenden Strafverfolgungsinteressen und den Geheimhaltungsinteressen.[667] Im Ergebnis können sowohl die Durchführung der Überwachungsmaßnahme als auch die hierbei erzielten Erkenntnisse geheim bleiben.

---

665 Zur Vergleichbarkeit mit dem Ermittlungsverfahren siehe *Thaman,* in: Perron, S. 534.

666 Vgl. *Kris/Wilson,* § 29:2, S. 226f.

667 50 U.S.C. § 1801 spricht von "to allow"; a.A. *Chiarella/Newton,* Army Law. (25) 1997, S. 27 Fn. 16.

Abseits des FISA richtet sich der Verbleib geheimdienstlich gewonnener Erkenntnisse unter anderem nach den Vorgaben der Mukasey Guidelines.[668] Die zu Strafverfolgungszwecken enthaltenen Übermittlungsregeln sind als Sollensvorschriften ausgestaltet und sehen daher im Grundsatz eine Zugänglichmachung strafrechtlich relevanter Erkenntnisse vor.[669] Allerdings begründen die Regelungen keine Offenlegungspflicht, sodass eine Zurückhaltung aus ermittlungstaktischen Gründen ebenfalls möglich ist.

(2) Auswirkungen auf das Strafverfahren

Bei einem Verbleib der Information im Geheimdienstsektor muss der Staat beim Fehlen sonstiger belastender Erkenntnisse grundsätzlich auf strafverfolgende Maßnahmen verzichten. Bei einer Vorenthaltung entlastenden Beweismaterials sind jedoch die Besonderheiten des *prosecution team standards* und des *availability* beziehungsweise *accessibility standards* zu berücksichtigen. Nach dem *prosecution team standard* betreffen die Offenlegungspflichten nicht allein die Staatsanwaltschaft, sondern gelten für sämtliche Behörden, die mit der Staatsanwaltschaft zusammenarbeiten.[670] Wie bereits im Rahmen der Übermittlungsproblematik dargestellt, können die Geheimdienste selbst aktiv die Ermittlungen der Strafverfolgung unterstützen. In diesem Fall sind die Geheimdienste nach Ansicht der Rechtsprechung als Teil des „Strafverfolgungsteams“ anzusehen. Da die Dienste insofern als Quasi-Strafverfolgungsbehörden fungieren, sind sie ebenfalls in die Offenlegungspflichten der *Brady Rule* mit einzubeziehen.[671] Eine Unterscheidung zwischen den verschiedenen Regierungsbehörden wird von der Rechtsprechung abgelehnt.[672] Eine solche aktive Kooperation ist vor allem im Bereich der Terrorbekämpfung

---

668 Speziell für FBI-Ermittlungen im Bereich des internationalen Terrorismus vgl. *Villaverde,* Cornell L. Rev. (88) 2003, S. 1516.

669 Mukasey Guidelines von 2008 unter Punkt VI.C.1, S. 36: “the agent shall present the relevant facts to the appropriate federal prosecutor”.

670 Vgl. *United States v. Brooks*, 966 F.2d 1500, 1503 (D.C. Cir. 1992): “For purposes of the *Brady Rule*, the prosecution has a duty to search files maintained by branches of government ‘closely aligned with the prosecution’.” Vgl. zudem *Baker,* Foreign Policy Winter 1994–1995, S. 45; *Fredman,* Yale L. & Pol’y Rev. (16) 1998, S. 347; *Manget,* Stan. L. & Pol’y Rev. (17) 2006, S. 422f; *Maxwell/Cline,* Los Angeles Lawyer (29) 2006, S. 38; *Villaverde,* Cornell L. Rev. (88) 2003, S. 1494ff, 1524; *Zabel/Benjamin,* S. 96.

671 Die Einbeziehung ist aber nicht unumstritten, da der *Supreme Court* die Entscheidung den unteren Gerichten überlassen hat; vgl. *Chesney,* in: Commission of Inquiry, S. 114; *Fredman,* Yale L. & Pol’y Rev. (16) 1998, S. 346f, 348; *Villaverde,* Cornell L. Rev. (88) 2003, S. 1494ff.

672 Siehe *United States v. Antone*, 603 F.2d 566, 569 (5th Cir. 1979): “this Court has declined to draw a distinction between different agencies under the same government, focusing instead upon the ‘prosecution team’ which includes both investigative and prosecutorial personnel”. Ebenso *United States v. Wood*, 57 F.3d 733, 737 (9th 1995); vgl. insgesamt *Chesney,* in: Commission of Inquiry, S. 114; *Villaverde,* Cornell L. Rev. (88) 2003, S. 1494, 1495 m.w.N.

und des internationalen Drogenhandels denkbar. Werden in diesem Zusammenhang entlastende Erkenntnisse erzielt, können diese in einem Strafverfahren einer direkten Übermittlungs- und Offenlegungspflicht unterliegen.[673] Grundvoraussetzung ist jedoch, dass die aktive Beteiligung der Dienste überhaupt bekannt ist.

Der *availability* und der *accessibility standard* präzisieren die Reichweite des nach der *Brady Rule* erforderlichen Besitzverhältnisses und damit den Umfang der damit verbundenen Offenlegungspflichten. Maßgeblicher Anknüpfungspunkt für die Pflicht ist die Verfügbarkeit beziehungsweise Zugänglichkeit der Informationen. Eine Einbeziehung der Geheimdienste in die Offenlegungspflicht hängt dementsprechend davon ab, inwieweit die Staatsanwaltschaft auf geheimdienstliche Erkenntnisse zugreifen kann. Von einer entsprechenden Zugriffsmöglichkeit wird man zumindest in Bezug auf das FBI ausgehen können, das aufgrund seiner hybriden Struktur sowohl in den Geheimdienst- als auch den Strafverfolgungssektor eingebunden ist. In diesem Fall erstreckt sich die Pflicht zur Suche nach entlastenden Beweismitteln auch auf den Geheimdienstsektor.[674]

Die Erfüllung der beschriebenen Offenlegungspflichten kann die Verteidigung aufgrund umfassender geheimdienstlicher Datenmengen vor erhebliche Herausforderungen stellen. Die Anfrage kann auf Zugang zu *Brady*-Material zu einer Übermittlung des gesamten und vor allem ungefilterten Datenvolumens führen. In diesen Fällen wird die Verteidigung oftmals weder über die personellen noch die finanziellen Ressourcen verfügen, um die übermittelten Datenmengen kurzfristig ausreichend auf entlastendes Beweismaterial überprüfen zu können. Die extremen Ausmaße eines solchen Vorgangs werden beispielhaft am Fall *United States v. Stein* deutlich.[675] In diesem Verfahren stellte die Regierung über 20 Millionen Dokumentseiten und über 60 Zeugen zur Verfügung. Die Verteidigungskosten beliefen sich pro Angeklagtem auf sieben bis 24 Millionen Dollar.[676] In einem weiteren Verfahren waren sogar 21.000 Stunden Abhöraufzeichnungen, 550 Videoaufzeichnungen und 30 Festplatten zu sichten.[677] Um eine unsachgemäße Benachteiligung zu vermeiden, gewähren die Gerichte in derartigen Konstellationen einen zeitlichen Aufschub, wenn die Verteidigung ihrerseits ein entsprechendes Bemühen darlegt.[678] Dieser Aufschub kann sogar mehrere Monate betragen.[679]

---

673 Vgl. *Kris/Wilson,* § 2:15, S. 73; *Manget,* Stan. L. & Pol'y Rev. (17) 2006, S. 422f. Die in diesem Zusammenhang übermittelten Datenmengen können jedoch einen Umfang erreichen, der die Arbeit der Verteidigung zeitweise zum Erliegen bringt.

674 Vgl. *Villaverde,* Cornell L. Rev. (88) 2003, S. 1512ff.

675 Vgl. *United States v. Stein*, 495 F. Supp. 2d 390, 424 (S.D.N.Y. 2007).

676 Vgl. *Zabel/Benjamin,* Teil 1, Endnote 295.

677 Vgl. *United States v. al-Arian*, 267 F. Supp. 2d 1258, 1260 (M.D. Fla. 2003); *Zabel/Benjamin,* S. 96.

678 Im konkreten Fall waren es acht Monate; vgl. *Zabel/Benjamin,* S. 115. Allgemein zu dieser sog. *continuance* siehe *Perron,* Beweisantragsrecht, S. 438.

bb) Geheimhaltungsentscheidung der Regierung

Eine Geheimhaltung kann weiterhin auf der Initiative der Regierung beruhen. Eine solche Konstellation kommt in Betracht, wenn die sonstigen Verfahrensbeteiligten anderweitig von der Involvierung der Geheimdienste erfahren und auf eine Offenlegung relevanter Erkenntnisse drängen. In diesem Fall kann die Exekutive wichtige Angaben zu Quellen und Methoden der Informationsfindung als *classified* und damit geheimhaltungsbedürftig einstufen. Die Einstufungs- und damit Geheimhaltungsentscheidung kann je nach Sachverhalt zu einer vollständigen Geheimhaltung führen.[680]

(1) Voraussetzungen der Geheimhaltung

Grundlage einer *classification*-Entscheidung bilden primär die zu nationalen Sicherheitsfragen erlassenen *Executive Orders* (E.O.), die ihrerseits durch verschiedene Empfehlungen und Verwaltungsanordnungen ergänzt werden.[681] Vorliegend ist vor allem die E.O. 13526 mit dem Titel *Classified National Security Information* von Relevanz.[682]

Für eine *classification*-Entscheidung müssen verschiedene formelle und materielle Voraussetzungen erfüllt sein. Zuständig für eine Geheimhaltungsentscheidung ist grundsätzlich der Präsident, sein Stellvertreter, bestimmte Behördenleiter oder sonst vom Präsidenten ermächtigte Personen.[683] Die Delegation bedarf der Schriftform und darf bei der höchsten Geheimhaltungsstufe nur auf bestimmte hochrangige Personen erfolgen.[684] In der Einstufungsentscheidung müssen Angaben zur Person und Position des anordnenden Beamten sowie Anweisung zur künftigen Aufhebung der Geheimhaltung enthalten sein. Weiterhin ist eine Zuordnung

---

679 Vgl. zu den möglichen Datenmengen *United States v. al-Arian*, 267 F. Supp. 2d 1258, 1260ff (M.D. Fla. 2003), sowie *Zabel/Benjamin,* S. 115.

680 Vgl. *Carter*, S. 162.

681 Siehe Classified National Security Information, Final Rule vom 25.6.2010 unter 32 C.F.R. 2001, 75 Fed. Reg. 37254, 28.6.2010, abrufbar unter www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf; das präsidiale Memorandum Implementation of the Executive Order, "Classified National Security Information" vom 29.12.2009, 75 Fed. Reg. 735, 5.1.2010, abrufbar unter www.archives.gov/isoo/pdf/implementing-memo.pdf und die Verwaltungsanordnung "Original Classification Authority" unter www.archives.gov/isoo/pdf/oca.pdf [jeweils Stand 1.5.12].

682 Vgl. E.O. 13526, Classified National Security Information vom 29.12.2009, 75 Fed. Reg. 707, 5.1.2010, abrufbar unter www.archives.gov/isoo/pdf/cnsi-eo.pdf [Stand 1.5.2012]. Davor waren die E.O. 12958; 13292 maßgeblich; vgl. *Elsea,* CRS 2011, Zusammenfassung; *Kosar,* CRS 2010, S. 3.

683 E.O. 13526 von 2009 unter Punkt 1.3.

684 E.O. 13526 von 2009 unter Punkt 1.3(c)(2).

zu den Geheimhaltungsstufen *top secret, secret* oder *confidential* erforderlich.[685] Die Entscheidung muss in regelmäßigen Zeitabschnitten überprüft werden.[686]

In materieller Hinsicht muss sich die *classification*-Entscheidung auf einen tauglichen Gegenstand beziehen, einem ausreichenden Geheimhaltungsgrund dienen, auf Ausnahmefälle begrenzt sein und keinem Ausschlusstatbestand unterliegen. Erste Voraussetzung ist das Vorliegen eines tauglichen Geheimhaltungsgegenstandes. Hiervon sind Informationen erfasst, die sich im Besitz oder unter der Kontrolle der Regierung befinden oder von einer ihrer Behörden erhoben wurden.[687]

Zweite Voraussetzung ist das Bestehen eines ausreichenden Geheimhaltungsgrundes. Die in der E.O. 13526 aufgelisteten *classification categories* bejahen die Geheimhaltungsbedürftigkeit bei Informationen im Zusammenhang mit Militäroperationen, ausländischen Regierungen, Massenvernichtungswaffen oder geheimdienstlichen Aktivitäten, Quellen und Methoden.[688] Ein ausreichender Geheimhaltungsgrund ist gegeben, wenn die unbefugte Offenlegung der Information eine Beeinträchtigung der nationalen Sicherheit beziehungsweise der Verteidigung gegen den transnationalen Terrorismus befürchten lässt.[689] Erfasst werden unter anderem Nachteile in Bezug auf die Landesverteidigung oder die auswärtigen Beziehungen. Bei der Beurteilung des Schadens sind die Sensibilität, der Wert, die Nutzbarkeit und die Herkunft der Informationen zu berücksichtigen.[690] Auf subjektiver Seite sind vernünftige Gründe für eine solche Beeinträchtigung erforderlich.

Als dritte Voraussetzung ist die Geheimhaltungsentscheidung auf wenige Ausnahmen zu begrenzen. Bestehen Zweifel, muss eine Einstufung unterbleiben oder die Information einer geringeren Geheimhaltungsstufe zugeordnet werden.[691] Geheimdienstrelevante Sachverhalte werden ausdrücklich als geheimhaltungsbedürftig anerkannt.

---

685 E.O. 13526 von 2009 unter Punkt 6.1(t).

686 E.O. 13526 von 2009 unter Punkt 1.9.

687 E.O. 13526 von 2009 unter Punkt 1.1.(a)(2): "the information is owned by, produced by or for, or is under the control of the United States Government".

688 E.O. 13526 von 2009 unter Punkt 1.1.(a)(3), 1.4. sowie insbesondere 1.4.(c): "intelligence activities (including covert action), intelligence sources or methods, or cryptology".

689 E.O. 13526 von 2009 unter Punkt 1.1.(a)(4): "unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism".

690 E.O. 13526 von 2009 unter Punkt 6.1.(l): "Damage to the national security means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information."

691 E.O. 13526 von 2009 unter Punkt 1.1.(b): "If there is significant doubt about the need to classify information, it shall not be classified."

Viertens darf die Geheimhaltungsentscheidung keinem der verschiedenen Ausschlusstatbestände beziehungsweise Verbote unterliegen. Eine Einstufung unterbleibt etwa, wenn durch diese Gesetzesverstöße, Ineffektivität oder Verwaltungsfehler vertuscht werden sollen.[692] Sind die genannten Voraussetzungen erfüllt, kann die Information einer der genannten Geheimhaltungsstufen zugeordnet werden.

(2) Auswirkungen auf das Strafverfahren

Mit einer *classification*-Entscheidung sind unterschiedliche Konsequenzen verbunden. Primäre Folge ist zunächst die Pflicht der verwahrenden Behörde, die als geheimhaltungsbedürftig eingestuften Informationen zu schützen.[693] Zur Umsetzung dieses Schutzes erlassen die Behörden eigenständige Verfahrensregeln. Der Zugriff auf die Informationen ist in diesem Fall an bestimmte Vorgaben gebunden.[694] Ob der Informationszugriff im Einzelfall tatsächlich gewährt wird, liegt im Ermessen der verwahrenden Stelle, sodass die Letztentscheidungsbefugnis letztlich bei der Exekutive beziehungsweise den Geheimdiensten verbleibt.[695] Die Entscheidung für eine vollumfängliche Geheimhaltung ist grundsätzlich bindend und kann weder durch den Betroffenen noch durch die Gerichte geändert werden.[696] Die Erkenntnisse bleiben dann sowohl gegenüber dem Betroffenen als auch gegenüber dem Richter geheim. In diesem Fall kommen weder die Verfahrensmechanismen des CIPA noch des FISA zur Anwendung. Diese greifen erst, wenn die Erkenntnisse zumindest dem Richter zur Überprüfung vorgelegt werden und dieser eine Ersetzung durch Beweissurrogate prüfen kann. Unterbleibt diese ebenfalls, muss in letzter Konsequenz von einer Strafverfolgung abgesehen werden.[697]

Allerdings kann diese Geheimhaltung auch entlastendes Beweismaterial betreffen. Um in diesen Fällen eine zu ausufernde Geheimhaltung zu verhindern, werden die Geheimhaltungsstufen regelmäßig kontrolliert.[698] In diesem Zusammenhang wird allerdings die Gefahr der sogenannten *overclassification,* das heißt einer zu leichtfertigen Geheimhaltungseinstufung, kritisiert. Danach würden die zuständigen

---

[692] E.O. 13526 von 2009 unter Punkt 1.7.(a): "In no case shall information be classified […] in order to conceal violations of law, inefficiency, or administrative error."

[693] Vgl. *Kosar,* CRS 2010, S. 16.

[694] Vgl. E.O. 13526 von 2009 unter Punkt 4.1 sowie *Carter*, S. 219.

[695] Vgl. *Kris/Wilson,* § 25:3, S. 127.

[696] Vgl. *United States v. Smith*, 750 F.2d 1215, 1217 (4th Cir. 1984). Darin heißt es: "the government pursuant to the authority mentioned in section 1 may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it". Ebenso *United States v. Musa*, 833 F. Supp. 752, 755 (E.D.Mo. 1993): "The determination whether to designate information as classified is a matter committed to the executive branch."

[697] Vgl. *Liu/Garvey,* CRS 2012, S. 1.

[698] So etwa im dritten Teil der E.O. 13526.

Stellen sicherheitsbezogene Informationen voreilig oder zu umfassend als geheimhaltungsbedürftig einstufen.[699]

b) Während der Hauptverhandlung

Geheimdienstinformationen können bei einer Involvierung nationaler Sicherheitsinteressen entsprechend den vorherigen Ausführungen allen Verfahrensbeteiligten gegenüber vorenthalten werden. Verzichtet die Exekutive in diesem Zusammenhang sogar auf eine Offenlegung gegenüber dem Richter, wird beim Fehlen anderweitiger Beweismittel entweder von der Einleitung eines Strafverfahrens abgesehen oder dieses eingestellt. Die Regierung wird von einer vollständigen Geheimhaltung daher nur Gebrauch machen, wenn sie ohnehin keine Strafverfolgung anstrebt.

2. Strategie der Richterbeteiligung

Bei der zweiten Geheimhaltungsstrategie werden die Geheimdienstinformationen ausschließlich dem Richter vorgelegt.

a) Vor der Hauptverhandlung

Eine im Vorfeld der Hauptverhandlung zum Schutz nationaler Sicherheitsinteressen auf den Richter beschränkte Offenlegung ist nach dem CIPA, den FRCRimP und dem FISA möglich.[700]

aa) Geheimhaltung nach dem CIPA

Eine in der *discovery*- beziehungsweise *disclosure*-Phase allein durch den Richter vorgenommene Relevanzprüfung wird nach 18 U.S.C. app. § 4 (Abk. § 4 CIPA) gestattet.[701] Diese Geheimhaltungsvariante betrifft die sogenannten *outsider cases*, in denen ausschließlich die Regierung über die geheimhaltungsbedürftigen Informationen verfügt.[702]

---

[699] Vgl. *Turner/Schulhofer,* S. 32f; *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1081.

[700] Die Anklageüberprüfung der *grand jury* erfolgt ebenfalls *ex parte*, vgl. Rule 6 FRCrimP; *Thaman,* in: Perron, S. 498ff; *Trüg,* S. 44. Diese Geheimhaltung beruht nicht auf nationalen Sicherheitsinteressen und bleibt vorliegend außer Betracht.

[701] 18 U.S.C. app. § 4; vgl. *Turner/Schulhofer,* S. 21; *Zabel/Benjamin,* S. 98.

[702] Vgl. *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1068.

(1) Voraussetzungen einer Geheimhaltung

Die maßgebliche Geheimhaltungsentscheidung beruht erneut auf der beschriebenen *classification*, die unter Beachtung der E.O. 13526 zustande gekommen sein muss. Der CIPA regelt den sich daran anschließenden verfahrensrechtlichen Umgang mit den *classified information.* Nach § 4 CIPA prüft der Richter *in camera* und *ex parte*, ob eine Offenlegung des als geheimhaltungsbedürftig eingestuften Materials erforderlich ist und wie diese konkret erfolgen könnte.[703]

Formelle Voraussetzung dieser Überprüfung ist ein schriftlicher Antrag der Regierung, in dem sie die Überprüfung unter Ausschluss der Öffentlichkeit und des Angeklagten verlangen muss.[704] Konkret kann dieser Antrag auf Durchführung eines *ex parte*-Verfahrens von jedem Staatsanwalt als Vertreter der Exekutive gestellt werden. Eine Festlegung auf hochrangige Beamte ist nicht vorgesehen.[705] Da die Anwendung des CIPA zunächst jedoch das Vorliegen einer offiziellen *classification* voraussetzt, ist diese umfassende Anordnungskompetenz unbedenklich.[706]

Inhaltlich nimmt das Gericht eine mehrstufige Prüfung vor. In dieser überprüft es zunächst das Bestehen der Offenlegungspflicht sowie im Anschluss die Ersetzbarkeit der offenzulegenden Informationen durch Beweissurrogate. Entsprechend dieser Prüfungsreihenfolge muss das Gericht auf einer ersten Stufe klären, ob die Regierung grundsätzlich zur Offenlegung verpflichtet ist. Die zu berücksichtigenden Offenlegungspflichten beziehen sich nach dem Wortlaut des § 4 CIPA auf die nach den FRCrimP offenzulegenden Dokumente und damit auf die in *Rule* 16 FRCrimP bestehenden Vorgaben.[707] Überwiegend wird die Vorschrift zusätzlich analog auf Zeugenaussagen[708] sowie *brady*-Material[709] angewandt. In dem für die Militärkommissionen maßgeblichen CIPA-Äquivalent ist die Anwendbarkeit auf Zeugenaussagen sogar ausdrücklich vorgesehen.[710]

---

[703] Im Anwendungsbereich des CIPA ist diese Verfahrensgestaltung fakultativ, während sie im Bereich der Militärkommissionen obligatorisch ist. Siehe 18 U.S.C. app. § 4 ("may permit") im Vergleich zu 10 U.S.C. § 949p-4(b)(2) ("shall").

[704] 18 U.S.C. app. § 4. Dieser Antrag wird dem Gericht üblicherweise unter Ausschluss der sonstigen Verfahrensbeteiligten übermittelt, vgl. *Kris/Wilson,* § 24:7.

[705] Vgl. hierzu *Kris/Wilson,* § 26:8, S. 167.

[706] Diese *classification* ist gerade auf wenige und hochrangige Vertreter begrenzt.

[707] 18 U.S.C. app. § 4: "The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure"; vgl. *Kris/Wilson,* § 24:7.

[708] Vgl. *United States v. Moussaoui*, 333 F.3d 509, 513ff (4th Cir. 2003), bestätigt in *United States v. Moussaoui*, 591 F.3d 263, 288 (4th Cir. 2010); vgl. insgesamt *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 48 Fn. 139.

[709] Vgl. *Kris/Wilson,* § 24:7.

[710] Vgl. 10 U.S.C. § 949p-4(b).

Der Richter prüft neben der Anwendbarkeit, inwiefern die als geheimhaltungsbedürftig eingestuften Informationen für die Verteidigung relevant beziehungsweise erheblich sind. In diesem Zusammenhang wird mehrheitlich betont, dass der CIPA die an die Offenlegung zu stellenden Anforderungen nicht ändert.[711] Im Widerspruch dazu hat sich in der Rechtsprechung jedoch ein sogenanntes *classified information privilege* beziehungsweise eine Art *balancing test* durchgesetzt.[712] Darin werden die nationalen Sicherheitsinteressen dem Interesse des Angeklagten am Erhalt der Information gegenübergestellt.[713] Für die Bejahung der Relevanz muss der Angeklagte darlegen, dass die Information zur Wahrnehmung seiner Verteidigungsinteressen hilfreich ist.[714] Hierdurch werden entgegen der vorgenannten Prämisse die Anforderungen an die Relevanzprüfung und damit an die Offenlegung erhöht.[715]

Diese Anforderungen werden zum Teil als ungerecht empfunden. Da im Anwendungsbereich des § 4 CIPA die gesamte Überprüfung unter Ausschluss der Verteidigung erfolge, habe der Angeklagte kaum eine Möglichkeit, die von der Regierung vorgebrachten Argumente zu entkräften.[716] Der Verteidiger könne mangels ausreichender Zugangsmöglichkeiten die Relevanz des Beweismittels nur auf abstrakte Mutmaßungen stützen, wovon sich das Gericht nur in wenigen Fällen überzeugen ließe.[717] Umgekehrt sei der Richter ohne den Input der Verteidigung oftmals nicht in der Lage, die Bedeutung bestimmter Erkenntnisse für die Verteidigung korrekt zu beurteilen.[718] Nach Ansicht der Kritiker ist es daher nicht unwahrscheinlich, dass für die Verteidigung relevantes Material nicht als solches erkannt und daher nicht offenlegt wird. Die allein durch den Richter vorgenommene Prüfung könne daher den Ausschluss der Verteidigung nicht ausreichend kompensieren.[719]

Bejaht das Gericht die Relevanz, prüft es in einem nächsten Schritt die Ersetzbarkeit der relevanten Information durch Beweissurrogate. Die Beweislast wechselt auf die Regierung, welche hinreichende Gründe dafür vorlegen muss, warum die Ersetzung der geheimhaltungsbedürftigen Information notwendig ist.[720] Hierzu muss sie den Nachweis erbringen, dass durch die Offenlegung nationale Sicher-

---

711 Vgl. *Zabel/Benjamin,* S. 98. Zu der entsprechenden Abwägung im Rahmen der *discovery* vgl. *Salgado,* Yale L. J. (98) 1988, S. 432, 439.

712 Vgl. hierzu *Shea,* Am. Crim. L. Rev. (27) 1990, S. 693f.

713 Vgl. *United States v. Smith* 750 F.2d 1215, 1218 (4th Cir. 1984); *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988).

714 Vgl. *United States v. Yunis* 867 F.2d 617, 623 (D.C. Cir. 1989) m.w.N.

715 Vgl. *Maxwell/Cline,* Los Angeles Lawyer (29) 2006, S. 38.

716 So *Kris/Wilson,* § 24:7.

717 Vgl. hierzu *Turner/Schulhofer,* S. 26.

718 Vgl. *Litt/Bennett,* in: Wittes, S. 156.

719 So *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1072.

720 Vgl. *Kris/Wilson,* § 24:7. § 4 CIPA spricht von "sufficient showing".

heitsinteressen gefährdet werden und andere Schutzvorkehrungen nicht ausreichen.[721] Der Schutz geheimdienstlicher Ermittlungsmethoden wurde von den Gerichten in diesem Kontext als schützenswertes Interesse anerkannt.[722] Im Geltungsbereich der Militärkommissionen ist der Quellen- und Methodenschutz sogar ausdrücklich in 10 U.S.C. § 949p-6(c)(2) des CIPA-Äquivalents vorgesehen.

Zusätzlich zu den in § 4 CIPA genannten Voraussetzungen ziehen die Gerichte bei der Entscheidung über die Beweissurrogation analog die Voraussetzungen von § 6(c) CIPA heran.[723] Danach ist eine Ersetzung durch Beweissurrogate nur zulässig, wenn diese dem Angeklagten die gleichen Verteidigungsmöglichkeiten bieten, die auch bei einer Offenlegung der geheimhaltungsbedürftigen Information selbst bestanden hätten.[724] Diese Voraussetzung wird in der Praxis bereits als erfüllt angesehen, wenn durch die Ersetzung keine unmittelbar verteidigungsrelevanten Informationen vorenthalten werden.[725] Eine Offenlegung ist daher nur geboten, wenn die fraglichen Informationen für die Verteidigung unentbehrlich sind. Die Darlegung einer bloßen theoretischen Relevanz genügt nicht.[726] Letztlich nehmen die Gerichte im zweiten Prüfungsschritt eine Abwägung zwischen der Bedeutung des Beweismittels für den Angeklagten und der Sensibilität der geheimhaltungsbedürftigen Information vor.[727]

(2) Auswirkungen auf das Strafverfahren

Je nach Sachverhalt werden an das Durchlaufen des CIPA-Verfahrens unterschiedliche Rechtsfolgen geknüpft. Bejaht der Richter sowohl die Geheimhaltungsbedürftigkeit, die Relevanz als auch die Ersetzbarkeit der Information, darf die Regierung die fraglichen Erkenntnisse durch drei gesetzlich normierte Beweissurrogate ersetzen.[728] Zur Auswahl stehen die Löschung der geheimhaltungs-

---

721 Vgl. *Kris/Wilson,* § 24:7. Der Nachweis entspricht zugleich den an die *classification* zu stellenden Mindestanforderungen.

722 Vgl. zur Schutzbedürftigkeit *Boumediene v. Bush*, 553 U.S. 723, 796 (S. Ct. 2008); sinngemäß *United States v. Scarfo*, 180 F. Supp. 2d 572, 575 (D.N.J. 2001), sowie *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989).

723 Vgl. *Turner/Schulhofer,* S. 21, S. 86 Fn. 40.

724 Vgl. *Chesney,* in: Commission of Inquiry, S. 109; *Liu/Garvey,* CRS 2012, S. 6; *Thaman,* in: Perron, S. 527.

725 Vgl. *Turner/Schulhofer,* S. 21.

726 *United States v. Smith*, 750 F.2d 1215, 1219 (4th Cir. 1984), *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989); vgl. *Turner/Schulhofer,* S. 21.

727 Vgl. *Kris/Wilson,* § 24:7. In Militärkommissionen genügen für die Ersetzbarkeit von *classified information* grundsätzlich die Zulässigkeit und Glaubwürdigkeit des Beweissurrogats. Siehe zum konkreten Verfahren 10 U.S.C. § 949p-6(d).

728 Siehe § 4 CIPA: "The court […] may authorize the United States to delete specified items of classified information from documents […], to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts

bedürftigen Passagen, die Substitution durch zusammenfassende Darstellungen oder das Zugeständnis der von der Verteidigung unter Beweis zu stellenden Behauptung.[729] In allen drei Varianten erhält die Verteidigung zu keinen Zeitpunkt Zugang zu den originären Dokumenten.

Verneint das Gericht die Ersetzbarkeit, muss die Regierung entweder die geheimhaltungsbedürftigen Informationen offenlegen oder vollständig auf die Einführung der Erkenntnisse verzichten. Die Kompetenz zur Entscheidung, ob es zu einer späteren Offenlegung des unmittelbaren Beweismittels oder einer Beweissurrogation kommt oder nicht, verbleibt damit bei der Exekutive. Die endgültige Geheimhaltungsentscheidung erfolgt durch den *Attorney General* per eidesstattlicher Erklärung. An diese Entscheidung ist selbst das Gericht gebunden, welches die Regierung nicht zur Aufhebung der Geheimhaltungsstufe zwingen kann.[730] Umgekehrt muss die Regierung jedoch die durch das Gericht auferlegten Sanktionen akzeptieren.[731] Diese Sanktionen sind erneut in analoger Anwendung dem § 6 CIPA zu entnehmen.[732] Danach müssen bei einer gerichtlich nicht gebilligten Geheimhaltung entweder die Anklage ganz oder teilweise fallen gelassen, die ausgeschlossenen Erkenntnisse als wahr unterstellt oder die Zeugenaussagen ausgeschlossen werden.[733] Die Entscheidung über die Ersetzbarkeit beziehungsweise Sanktionierung ist nicht endgültig, sondern kann von der Regierung nach § 7 CIPA in einem Zwischenverfahren erneut überprüft werden.[734]

Das für eine Geheimhaltung nach dem CIPA vorgesehene Surrogations- und Kompensationsmodell wird von der Praxis unterschiedlich beurteilt. Insbesondere die durch die Beweissurrogation eröffneten Möglichkeiten werden vonseiten der Verteidigung nicht immer als ausreichend erachtet. Da die Verteidigung das stellvertretend eingeführte sekundäre Beweismittel nicht in gleicher Weise auf seine Glaubwürdigkeit und Aussagekraft testen könne, sei nach Ansicht einiger Kritiker die Vereinbarkeit mit den adversatorischen Grundstrukturen zweifelhaft.[735] Die nachteiligen Auswirkungen würden an Verfahren deutlich, in denen die Verteidigung mangels Möglichkeit zum Kreuzverhör nicht auf Täuschungs- beziehungs-

---

that the classified information would tend to prove." Vgl. *Chesney,* in: Commission of Inquiry, S. 109; *Thaman,* in: Perron, S. 512.

729 Vgl. *Thaman,* in: Perron, S. 526.

730 Sog. *declassification*; vgl. *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1069.

731 Vgl. *Thaman,* in: Perron, S. 526.

732 Genauer dem 18 U.S.C. app. § 6(e)(2), vgl. zudem *Chesney,* in: Commission of Inquiry, S. 109.

733 Vgl. *Thaman,* in: Perron, S. 526. Als Kompromiss kommt der Erlass einer sog. *protective order* in Betracht; vgl. hierzu Konstellation 3 unter Teil 3, IV.B.3.

734 Nach *Turner/Schulhofer,* S. 29, ist bislang jedoch kein Fall bekannt, in dem die Ersetzbarkeit der als geheimhaltungsbedürftig eingestuften Informationen abgelehnt wurde.

735 So *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1074f.

weise Betrugshandlungen oder Eigeninteressen des Zeugen hinweisen konnte.[736] Zudem sei die Lösung in praktischer Hinsicht schwer umsetzbar, da die Einschätzung vergleichbarer Verteidigungsmöglichkeiten als Prognoseentscheidung stets mit vielen Unsicherheiten behaftet sei. Umgekehrt führen die Befürworter diese Unsicherheiten gerade als Beleg für die Vorteile einer Beweissurrogation an. Eine Protokollverlesung sei insofern viel berechenbarer als eine Zeugenvernehmung.[737]

Demgegenüber werden die vorgesehenen Sanktionsmechanismen überwiegend als positiv beurteilt. Insbesondere die vorgesehene Einstellung einzelner Anklagepunkte könne die Nachteile einer Geheimhaltung zumindest teilweise kompensieren. Die ebenfalls mögliche Wahrunterstellung wird demgegenüber kritisch gesehen, da die Regierung durch das Zugeständnis der unter Beweis zu stellenden Tatsachen die unmittelbare Präsentation eines Beweismittels verhindern könne. Dies sei bedenklich, da die Wirkung einer solchen Feststellung weit hinter dem Effekt einer unmittelbar vor den Geschworenen erfolgenden Zeugenaussage zurückbleibe.[738] Da keine offiziellen Statistiken zur Anzahl und Gestaltung von CIPA-Verfahren existieren, kann die praktische Relevanz dieses Kompensationsmodells nicht beurteilt werden.[739]

Die geringen nachträglichen Kontrollmöglichkeiten werden wiederum als Nachteil dieser Geheimhaltungsstrategie empfunden. Die Kritiker führen an, dass die Geheimhaltungsentscheidung der Exekutive mit der *review* beziehungsweise *declassification* lediglich internen Kontrollmechanismen unterliege.[740] Außerhalb dieser Regelungen sei eine endgültige Geheimhaltungsentscheidung der Exekutive nicht aufhebbar. Zudem sei eine Überprüfung der Beweissurrogation im Strafverfahren nach § 7 CIPA der Regierung vorbehalten, ohne dass dem Betroffenen vergleichbare Rechtsschutzmöglichkeiten zuständen.[741]

bb) Geheimhaltung nach dem FISA

Die bei einer Nutzung von FISA-Erkenntnissen erforderliche Relevanz- und Zulässigkeitsprüfung kann ebenfalls auf den Richter begrenzt werden.[742]

---

736 Zu dieser Kritik vgl. *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1076.

737 So *Zabel/Benjamin,* S. 94.

738 So *Perron,* Beweisantragsrecht, S. 468.

739 Vgl. hierzu *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1085.

740 Siehe hierzu den fünften Teil der E.O. 13526.

741 Vgl. *Shea,* Am. Crim. L. Rev. (27) 1990, S. 665.

742 Vgl. hierzu 50 U.S.C. § 1806(f), § 1825(g), § 1845 (f)(1). Der Richter gehört jedoch nicht dem FISC, sondern dem jeweils zuständigen Bezirksgericht *(district court)* an.

(1) Voraussetzungen einer Geheimhaltung

Voraussetzung für die Gestaltung als *in camera ex parte*-Verfahren ist eine Erklärung des *Attorney General*, in welcher er die Geheimhaltungsbedürftigkeit der Vorgänge beziehungsweise eine Bedrohung der nationalen Sicherheit eidesstattlich versichert.[743] Eine solche Erklärung wurde bisher in allen bekannten Verfahren abgegeben.[744] Zwar sieht das Gesetz theoretisch eine Beteiligung des Angeklagten vor, wenn diese für eine Beurteilung der Rechtmäßigkeit notwendig ist,[745] bislang wurde eine solche Einbeziehung des Angeklagten jedoch von keinem Gericht für notwendig erachtet.[746] Damit erfolgt die Überprüfung von FISA-Vorgängen faktisch immer unter Ausschluss der Öffentlichkeit und der sonstigen Verfahrensbeteiligten.[747]

In verfahrensrechtlicher Hinsicht kann die FISA-Kontrolle durch drei Sachverhalte ausgelöst werden: erstens, wenn die Regierung FISA-Erkenntnisse zum Nachteil einer Person als Beweismittel nutzen möchte,[748] zweitens, wenn der Angeklagte einen Antrag auf Nichtzulassung der FISA-Erkenntnisse oder drittens einen Antrag auf Offenlegung der FISA-Vorgänge stellt. Bei den Anträgen des Angeklagten spricht das Gesetz insofern von der *motion to suppress* beziehungsweise der *motion to disclose the evidence obtained or derived*.[749] Diese Anträge dienen in der Regel dazu, die Zulassung der FISA-Erkenntnisse zu verhindern. Bei einem Antrag auf Nichtzulassung wird dieses Ziel direkt verfolgt. Bei einem Antrag auf Offenlegung der FISA-Vorgänge, das heißt den FISA-Antrag und dessen Durchführungsanordnung, wird dieses Ziel mittelbar erreicht.

Inhaltlich überprüft das Gericht die Rechtmäßigkeit der Anordnung und der Durchführung der FISA-Überwachung.[750] Der Geheimhaltung unterliegen hierbei

---

[743] 50 U.S.C. §§ 1806(f), 1825(g), 1845 (f)(1). Diese offene Erklärung wird in der Regel durch eine geheimhaltungsbedürftige Erklärung der Regierung ergänzt, in der ein hochrangiger Beamter die konkret aus der Offenlegung resultierende Bedrohung der nationalen Sicherheit vorträgt; vgl. *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006) bestätigt durch *United States v. Rosen*, 557 F.3d 192 (4th Cir. 2009); *United States v. Rahman*, 861 F. Supp. 247, 250 (S.D.N.Y. 1994); *Kris/Wilson,* § 30:7, S. 254f.

[744] Vgl. *Kris/Wilson,* § 30:3, S. 248; § 30:7, S. 254; *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1078 Fn. 77.

[745] 50 U.S.C. § 1806(f), § 1825(g), § 1845 (f)(1).

[746] Vgl. *Gurulé/Corn,* S. 237; *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 156f; *Kris/Wilson,* § 31:3, S. 264. Den genannten Autoren zufolge ist ein solcher Fall bislang nicht aufgetreten. Dort mit zahlreichen Nachweisen aus der Rechtsprechung.

[747] Vgl. *Kris/Wilson,* § 31:6, S. 271.

[748] Siehe zur Mitteilungspflicht 50 U.S.C. §§ 1806(c), (d), 1825(d), (e), 1845(c), (d) sowie *Kris/Wilson,* § 29:3.

[749] Siehe 50 U.S.C. §§ 1806(e), 1825(f), 1845(e). Der Antrag auf Offenlegung kommt in Betracht, wenn die Regierung angibt, trotz FISA-Überwachung keine FISA-Erkenntnisse heranzuziehen; vgl. hierzu *Gurulé/Corn,* S. 236ff.

[750] Vgl. *Maggs*, S. 237.

vor allem der FISA-Antrag und die FISA-Durchführungsanordnung, während die einzuführenden FISA-Erkenntnisse grundsätzlich zugänglich gemacht werden.[751] Wie bereits zuvor dargestellt, sind in diesem Verfahrensabschnitt sowohl die Einwirkungsmöglichkeiten des Angeklagten als auch die Prüfungskompetenzen des Gerichts schwach ausgebildet.[752] Der Angeklagte kann aufgrund seines Ausschlusses den Vorwurf rechtswidrigen Handelns meist nur auf abstrakte beziehungsweise theoretische Mutmaßungen stützen.[753] Das Gericht wiederum ist in seiner Prüfung an den Beurteilungs- und Ermessensspielraum der Exekutive gebunden und darf deren Einschätzungen nicht im Nachhinein ersetzen.[754] Die Kontrolle greift daher regelmäßig nur bei offensichtlichen Fehlern.[755]

(2) Auswirkungen auf das Strafverfahren

Die an das Kontrollverfahren anknüpfenden Rechtsfolgen unterscheiden sich danach, welcher Antrag der Kontrolle zugrunde lag. Stellt das Gericht die Rechtswidrigkeit der Überwachung fest, werden die FISA-Erkenntnisse bei einem Antrag auf Nichtzulassung nicht als Beweismittel zugelassen.[756] Wird wiederum bei einem Antrag auf Offenlegung die Offenlegungspflicht bejaht, kann der Angeklagte die Überwachung in einem streitigen Verfahren überprüfen lassen.[757] Der mit dem Offenlegungsantrag angestrebte Zugang ist notwendig, um einen hinreichend begründeten Antrag auf Ausschluss des Beweismittels stellen zu können.[758] Gegen die Offenlegungsentscheidung beziehungsweise Nichtzulassungsentscheidung des Gerichts kann die Regierung einstweilen vorgehen.[759] Bejaht das Gericht demgegenüber die Rechtmäßigkeit der Überwachung, wird der Antrag des Angeklagten auf Nichtzulassung der Beweismittel abgelehnt. Dasselbe gilt für einen Antrag auf

---

751 Vgl. *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1078. Sind die FISA-Erkenntnisse selbst geheimhaltungsbedürftig, greift der CIPA. Vgl. zur Geheimhaltungsbedürftigkeit der FISA-Vorgänge *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990).

752 Siehe hierzu Teil 3, III.B.5.c)cc).

753 Vgl. *Kris/Wilson,* § 32:2, S. 281.

754 *United States v. Rahman*, 861 F. Supp. 247, 250 (S.D.N.Y. 1994); *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984), sowie *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1078.

755 Vgl. *Kris/Wilson,* § 30:5, S. 287ff.

756 Eine entsprechende Pflicht besteht bei 50 U.S.C. § 1806(g) *(electronic surveillance)* und § 1825(h) *(physical search)*: "shall […] suppress the evidence". Bei § 1845(g)(1) steht die Nichtzulassungsentscheidung im Ermessen des Gerichts – "may […] suppress".

757 Vgl. *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982); *Kris/Wilson,* § § 30:7, S. 255.

758 Vgl. *Gurulé/Corn,* S. 237.

759 Vgl. *Kris/Wilson,* § 33:2, S. 300f. Diese dem Wortlaut nicht entnehmbare Regelung wird historisch begründet. Die parallele Vorschrift bezüglich der Nichtzulassung strafrechtlicher Erkenntnisse findet sich in 18 U.S.C. § 3731.

Offenlegung der FISA-Vorgänge. Die Rechtmäßigkeitsentscheidung ist grundsätzlich bindend, sodass der Angeklagte im Anschluss keine Möglichkeit mehr hat, die Rechtmäßigkeit der Überwachung überprüfen zu lassen. Anders als nach Title III erhält der Angeklagte damit zu keinem Zeitpunkt Zugang zu den Ursprungsdokumenten.[760]

cc) Geheimhaltung nach dem *informer's privilege*

Nach dem sogenannten *informer's privilege* können schließlich sensible Informationen über Informanten oder Vertrauenspersonen geschützt werden.[761] Ist der Anwendungsbereich des *informer's privilege* eröffnet, werden die Anforderungen an die Relevanzprüfung erhöht, sodass die Erkenntnisse unter erleichterten Bedingungen geheim gehalten werden können.[762] Um dennoch eine Offenlegung zu erreichen, muss die Verteidigung in einem schriftlichen Antrag die Relevanz und Entscheidungserheblichkeit der geheim gehaltenen Informationen darlegen.[763] Daraufhin überprüft der Richter in Abwesenheit des Angeklagten, ob dessen Interessen die bestehenden Geheimhaltungsinteressen überwiegen.[764] Bei dieser Abwägung werden sowohl der persönliche Schutz des Zeugen als auch dessen künftige Verwendbarkeit berücksichtigt.[765] Eine Offenlegung scheidet beispielsweise aus, wenn der Informant keine konkreten Aussagen zum Tathergang, sondern nur allgemeine Angaben machen kann.[766] Die Verteidigung selbst kann lediglich durch die Vorlage von Fragenkatalogen auf die Entscheidung Einfluss nehmen. Im Vergleich zu den Regeln des CIPA spielt das *informer's privilege* nur eine untergeordnete Rolle.[767] Sobald die Verteidigung die Relevanz der zurückgehaltenen Informationen nachweisen kann, scheidet eine Geheimhaltung unter Rückgriff auf das *informer's privilege* aus.[768] Ihm kommt daher nur eine sehr geringe Schutzwirkung

---

760 Vgl. *Hall,* Wake Forest L. Rev. (41) 2006, S. 70; *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 154; *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1078. So wurde eine Einbeziehung in *United States v. Rahman*, 861 F. Supp. 247, 250 (S.D.N.Y. 1994) abgelehnt.

761 Vgl. *Roviaro v. United States*, 353 U.S. 53 (S. Ct. 1957); *Trüg,* S. 332, 333. Zur analogen Anwendbarkeit auf geheimdienstliche Quellen vgl. *Stacy,* U. Colo. L. Rev. (58) 1987, S. 192.

762 Vgl. *Turner/Schulhofer,* S. 18.

763 Vgl. *Thaman,* in: Perron, S. 525.

764 In diesem Zusammenhang wird zum Teil von einem *in camera*-Verfahren gesprochen. Entgegen dieser Bezeichnung wird jedoch nicht nur die Öffentlichkeit, sondern auch der Angeklagte ausgeschlossen. Vgl. zur Problematik *Thaman,* in: Perron, S. 526.

765 Zu diesem Zweck kann der Richter eine Anhörung unter Beteiligung der Staatsanwaltschaft und des Informanten durchführen, vgl. *Thaman,* in: Perron, S. 525f.

766 Vgl. *Trüg,* S. 333.

767 Vgl. zu den nachfolgenden Ausführungen *Turner/Schulhofer,* S. 20.

768 Vgl. *Trüg,* S. 333.

zu. Im Vergleich dazu gestattet der CIPA sogar die Zurückhaltung verteidigungsrelevanter Informationen, sofern das zur Verfügung gestellte Beweissurrogat zur Wahrung der Verteidigungsinteressen ausreichend ist.

dd) Geheimhaltung nach der Rule 16 FRCrimP

Eine weitere Geheimhaltungsmöglichkeit eröffnet die *Rule* 16 FRCrimP, welche in der *discovery*-Phase ebenfalls eine Beschränkung der Offenlegung auf den Richter gestattet. In diesem Verfahrensstadium legen die Verteidigung und die Staatsanwaltschaft soweit notwendig ihre Beweismittel vor. Um eine Offenlegung allein vor dem Richter zu ermöglichen, kann jede Partei den Erlass einer Schutzanordnung beantragen. Hierzu muss sie sich nach dem Gesetzeswortlaut auf einen *good cause* stützen können. Das Gericht überprüft daraufhin unter Ausschluss der Gegenpartei, ob und inwieweit die Akteneinsicht besteht.[769] Bei dieser Entscheidung steht dem Gericht ein gewisser Beurteilungsspielraum zu.[770] Der Schutz nationalen Sicherheitsinteressen wird als ausreichender Grund für eine Zugangsbeschränkung anerkannt, solange durch die Geheimhaltung das Recht des Angeklagten auf ein faires Verfahren nicht beeinträchtigt wird.[771] In der Praxis wird diese Vorschrift zum Schutz geheimhaltungsbedürftiger Informationen kaum herangezogen.[772] Diese Zurückhaltung beruht sowohl auf der im Vergleich zum CIPA größeren Abhängigkeit vom Gericht als auch dem Fehlen einer dem § 7 CIPA vergleichbaren Zwischenbeschwerde. Die Gefahr einer ungewollten Offenlegung oder Verfahrenseinstellung ist damit weitaus größer als nach dem CIPA. Dieses Risiko wird die Regierung nur in den wenigsten Fällen eingehen.[773]

ee) Zwischenergebnis

Im Vorverfahren kann die Offenlegung geheimhaltungsbedürftiger Informationen unter Berufung auf verschiedene Vorschriften auf den Richter beschränkt werden. In der Praxis spielen vor allem die Regeln des CIPA und des FISA eine bedeutsame Rolle.

---

[769] Rule 16(d)(1) FRCrimP: "At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief. The court may permit a party to show good cause by a written statement that the court will inspect ex parte." Vgl. *Kris/Wilson,* § 26:6, S. 152f.

[770] Rule 16(d)(1) FRCrimP spricht von "may".

[771] Vgl. *Kris/Wilson,* § 26:6, S. 152f.

[772] Vgl. *Hooper/Rauma/Leary/Thrope*, S. 36; *Kris/Wilson,* § 26:6, S. 153.

[773] So *Kris/Wilson,* § 26:6, S. 153.

b) Während der Hauptverhandlung

Bei einer in der Hauptverhandlung auf den Richter begrenzten Offenlegung ist zwischen dem körperlichen Ausschluss der Verteidigungsseite einerseits und der Vorenthaltung von Informationen andererseits zu differenzieren. Im CIPA ist grundsätzlich keine der beiden Konstellationen vorgesehen.[774] Indirekt kann jedoch zumindest die zweite Konstellation, das heißt die Geheimhaltung von Wissen, im Zusammenhang mit § 6 CIPA als mittelbare Folge einer Beweissurrogation nach § 4 CIPA zustande kommen. Um diese Geheimhaltungsvariante verstehen zu können, muss man sich zunächst die sonstigen Mechanismen des CIPA vor Augen führen. Das Verfahren nach § 6 CIPA schließt sich zeitlich an die Akteneinsicht nach § 4 CIPA an. Beide Verfahrensabschnitte werden vor dem eigentlichen Hauptverfahren durchgeführt.[775] Die Vorschrift des § 4 CIPA regelt, inwiefern Informationen im Besitz der Regierung im Vorverfahren gegenüber der Verteidigung offenzulegen sind. Nach § 6 CIPA wird wiederum festgelegt, welche Informationen konkret in der Hauptverhandlung präsentiert werden. Im Verfahren nach § 6 CIPA verfügt der Angeklagte entweder bereits aufgrund der selbstständigen Informationsbeschaffung oder infolge der Offenlegung nach § 4 CIPA über die maßgeblichen Informationen. Danach müsste die Einordnung in die vorliegende Fallgruppe eigentlich ausscheiden. Bei genauerer Betrachtung wird jedoch deutlich, dass einer Zulässigkeitsprüfung nach § 6 CIPA nur solche Informationen unterzogen werden können, die nach § 4 CIPA bereits offengelegt wurden. Wird also nach § 4 CIPA die Ersetzung durch Beweissurrogate gestattet, können auch nur diese in das Hauptverfahren eingeführt werden. Durch das Verfahren des § 4 CIPA liegt das Beweismittel bereits in einer Form vor, die einen ausreichenden Schutz der nationalen Sicherheitsinteressen gestattet. Für eine zusätzliche geheimhaltungsspezifische Überprüfung nach § 6 CIPA besteht in diesem Fall kein Bedarf.[776] Die Ersetzung im Rahmen des § 4 CIPA führt damit letztlich dazu, dass die geheimhaltungsbedürftigen Informationen über das Vorverfahren hinaus auch in der Hauptverhandlung geheim bleiben. Der Ausschluss des Angeklagten und seines Verteidigers wirkt damit bis in die Hauptverhandlung fort.

---

774 Vgl. zum körperlichen Ausschluss *Chesney,* in: Commission of Inquiry, S. 112f.

775 Vgl. *Kris/Wilson,* § 27:2, S. 172.

776 So *Kris/Wilson,* § 27:7, S. 192. Das Verfahren nach § 6 CIPA kommt nur zur Anwendung, wenn der Angeklagte bereits im Besitz der Information ist. Für einen Zugang zu geheimhaltungsbedürftigen Informationen ist allein § 4 CIPA maßgeblich, nicht § 6 CIPA.

3. Strategie der Verteidigerbeteiligung

Die dritte Geheimhaltungsstrategie betrifft die Nutzung von geheimhaltungsbedürftigen Informationen unter Ausschluss des Angeklagten bei gleichzeitiger Beteiligung seines Verteidigers.[777]

Historisch gesehen war in den ursprünglichen CIPA-Regeln von 1980 eine solche Geheimhaltungsmöglichkeit zunächst nicht vorgesehen. Vielmehr sollte das Gesetzeswerk lediglich der als *graymail* bekannten Erpressungspraxis entgegenwirken. Eine *graymail*-Situation trat typischerweise bei der Strafverfolgung von Spionen im Kalten Krieg auf, in welcher der Angeklagte aufgrund seiner beruflichen Stellung zuvor Zugang zu den geheimhaltungsbedürftigen Informationen hatte; etwa als Mitarbeiter eines Geheimdienstes. In diesen *insider cases* drohte der Angeklagte mit der Offenlegung geheimhaltungsbedürftiger Informationen, um den Staat zur Einstellung des Strafverfahrens zu bewegen.[778] Das damit auf staatlicher Seite verbundene Dilemma sollte durch die im CIPA geschaffenen Kontroll- und Surrogationsmöglichkeiten abgemildert werden. In der ursprünglichen Fassung sollte es damit vor allem eine Offenlegung gegenüber der Öffentlichkeit verhindern. Eine Geheimhaltung gegenüber dem Angeklagten war nicht notwendig, da dieser bereits Zugang zu den geheimhaltungsbedürftigen Erkenntnissen hatte.[779]

In der vorliegend zu untersuchenden Geheimhaltungsstrategie soll die Geheimhaltung allerdings auch und gerade gegenüber dem Angeklagten erfolgen. Eine solche Notwendigkeit besteht beispielsweise in Strafverfahren gegen mutmaßliche Terroristen, in denen es geheimdienstliche Informationsquellen und -methoden zu schützen gilt.[780] Die ursprünglich auf die *graymail*-Situation ausgerichteten Vorschriften wurden jedoch von den Gerichten auf die letztgenannte Konstellation ausgedehnt, sodass der CIPA auch im Rahmen der vorliegend zu untersuchenden Strategie der Verteidigerbeteiligung von Bedeutung ist.[781]

a) Vor der Hauptverhandlung

Eine auf den Verteidiger beschränkte Offenlegung kann die Regierung durch Beantragung einer sogenannten *protective order* nach § 3 CIPA erreichen.[782] Diese

---

[777] Diese Konstellation tritt weitaus seltener auf, da die Gerichte in der Regel auf eine Involvierung der Verteidigung verzichten, vgl. *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1068.

[778] Vgl. *Liu/Garvey,* CRS 2012, S. 1; *Zabel/Benjamin,* S. 9.

[779] Vgl. *Chesney,* in: Commission of Inquiry, S. 113.

[780] Vgl. *Chesney,* in: Commission of Inquiry, S. 113.

[781] Vgl. *United States v. Sterling*, Case No. 1:10-cr-485 (E.D. Va. 2011); *Liu/Garvey,* CRS 2012, S. 9f.

[782] 18 U.S.C. app. § 3: "Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United

ursprünglich auf räumliche Schutzvorkehrungen gemünzte Vorschrift wurde in richterlicher Rechtsfortbildung auf Fälle der vorliegenden Konstellation ausgedehnt.[783]

aa) Voraussetzungen einer Geheimhaltung

Mithilfe einer gerichtlichen Schutzanordnung kann die Offenlegung an das Durchlaufen einer Sicherheitsüberprüfung *(security clearance)* geknüpft werden. Dieses Erfordernis ist bei einem Verfahren vor einer Militärkommission unproblematisch, da der beizuordnende *military counsel* als Angehöriger des Militärs über das notwendige Sicherheitszertifikat verfügt.[784] In den zivilen Strafverfahren muss der Verteidiger demgegenüber vor einer Beteiligung zunächst eine Sicherheitsüberprüfung durchlaufen.[785] Da der Beschuldigte regelmäßig kein derartiges Sicherheitszertifikat erhalten wird, kann die Offenlegung der geheimhaltungsbedürftigen Informationen nur gegenüber dem sicherheitsgeprüften Verteidiger erfolgen.[786] Die in diesem Zusammenhang erhaltenen Erkenntnisse darf der Verteidiger nicht mit seinem Mandanten besprechen.[787] Wann genau eine solche Schutzanordnung erlassen werden darf, ist mangels eindeutiger gesetzlicher Normierung weitgehend unklar. Bisher haben die Gerichte eine Schutzanordnung nach einer Abwägung der staatlichen Geheimhaltungsinteressen mit den Verteidigungsinteressen des Beschuldigten erlassen.[788] Da in Terrorismusverfahren dem Geheimhaltungsinteresse ein hohes Gewicht zukommt, wird die Abwägung hier regelmäßig zu einem Ausschluss des Beschuldigten führen.

Im Anwendungsbereich des FISA kann ebenfalls eine Schutzanordnung erlassen werden. Hiervon ist beispielsweise auszugehen, wenn das Gericht eine Beteiligung

---

States to any defendant in any criminal case in a district court of the United States." Das Gesetz macht dementsprechend keine Vorgaben zur Ausgestaltung einer Schutzanordnung.

783 Räumliche Schutzvorkehrungen sind etwa das Verbringen an einen geschützten Aufbewahrungsort wie den *Sensitive Compartmented Information Facilities* (SCIF) innerhalb des Gerichtsgebäudes oder Zugangsbegrenzungen; vgl. *Maxwell/Cline,* Los Angeles Lawyer (29) 2006, S. 38.

784 Dies gilt zugleich für die Geschworenen, die ebenfalls dem Militär angehören.

785 Vgl. *Turner/Schulhofer,* S. 21, 25f. Zu den Besonderheiten einer Militärkommission vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 45 Fn. 130. Zur Beiordnung siehe 10 U.S.C. § 948k(a)(3). Eine solche Sicherheitsprüfung bzw. Ersetzung durch einen tauglichen, geprüften Verteidiger kann mehrere Wochen und Monate in Anspruch nehmen, vgl. *Maxwell/Cline,* Los Angeles Lawyer (29) 2006, S. 38.

786 Vgl. *Kris/Wilson,* § 26:4, S. 148f; *Turner/Schulhofer,* S. 21, 25ff; *United States v. Bin Laden*, 126 F. Supp. 2d 264, 287 (S.D.N.Y. 2000). Es wird allerdings betont, dass die Sicherheitsüberprüfung dem Verteidiger nicht zwingend den Zutritt zu sämtlichen Dokumenten verschafft; vgl. *United States v. Moussaoui*, 591 F.3d 263, 267 (4th Cir. 2010).

787 Vgl. hierzu *Liu/Garvey,* CRS 2012, S. 3; *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1070.

788 Vgl. *Kris/Wilson,* § 26:4, S. 150.

des Verteidigers bei der Rechtmäßigkeitskontrolle für notwendig erachtet. Seine Teilnahme erfolgt in diesem Fall unter strengen Sicherheits- und Geheimhaltungsvorkehrungen.[789]

bb) Auswirkungen auf das Strafverfahren

Kommt es zum Erlass einer *protective order,* erfolgt die Offenlegung geheimhaltungsbedürftigen Materials ausschließlich vor einem sicherheitsgeprüften Verteidiger.[790] Dieses Vorgehen wird von manchen Kritikern als Einschnitt in die Verteidigungsmöglichkeiten gewertet, da die Regierung dadurch faktisch ein Vetorecht hinsichtlich des gewählten Verteidigers erhalte. Die Gerichte haben dies allerdings als unbedenklich eingestuft, da durch die Verfassung nicht die Wahl eines bestimmten Verteidigers, sondern lediglich eine effektive Verteidigung garantiert werde.[791] Das Effektivitätserfordernis sei gewahrt, da der sicherheitsgeprüfte Verteidiger die Interessen des Beschuldigten in gleichwertiger Art und Weise vertreten könne. Die Einflussnahme auf die Wahlentscheidung selbst sei gerechtfertigt, da nur durch die Sicherheitsüberprüfung die erforderliche Glaubwürdigkeit und der notwendige Geheimnisschutz gewährleistet werden könnte.[792] Zudem verweisen die Gerichte auf die Vorteile der Schutzanordnung, da der Verteidiger anders als bei der Strategie der Richterbeteiligung nunmehr auf die Offenlegung entlastenden Beweismaterials hinwirken könnte.[793]

Wird die Schutzanordnung zusätzlich mit einem Sprechverbot verknüpft, können die Auswirkungen auf das Strafverfahren erheblich sein. Wird dem Verteidiger entsprechend dieser Vorgabe die Rücksprache mit seinem Mandanten verboten, kann er in aller Regel weder die Relevanz der vorgelegten Information richtig einschätzen noch seinen Mandanten ausreichend auf eine Zeugenaussage vorbereiten. Dieser Kritikpunkt wurde von der Rechtsprechung aufgenommen. Danach kann der Verteidiger die für den Erlass einer Schutzanordnung angeführten Gründe widerlegen. Hierzu muss er nachweisen, dass die (Wissens-)Beteiligung des Beschuldigten zur sachgemäßen Beurteilung erforderlich ist beziehungsweise die Tatsachen für die Verteidigung relevant sind.[794]

---

[789] Vgl. 50 U.S.C. § 1806(f): "under appropriate security procedures and protective orders"; vgl. zudem *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 157.

[790] Vgl. zu dieser Möglichkeit *United States v. Bin Laden,* 58 F. Supp. 2d. 113, 116 (S.D.N.Y. 1999), *Chesney,* in: Commission of Inquiry, S. 113; *Turner/Schulhofer,* S. 21; *Zabel/Benjamin,* S. 99.

[791] Vgl. *United States v. Bin Laden*, 58 F. Supp. 2d 113, 119 (S.D.N.Y. 1999), sowie *Maxwell/Cline,* Los Angeles Lawyer (29) 2006, S. 42 Fn. 11; *Perron,* Beweisantragsrecht, S. 415; *Shea,* Am. Crim. L. Rev. (27) 1990, S. 678; *Turner/Schulhofer,* S. 26.

[792] Vgl. *Kris/Wilson,* § 26:4, S. 150.

[793] Vgl. zu diesem Argument *Turner/Schulhofer,* S. 26.

[794] Vgl. *Liu/Garvey,* CRS 2012, S. 3f; *Turner/Schulhofer,* S. 28.

Bei dieser Geheimhaltungsvariante sind zudem die Fälle zu bedenken, in denen der Beschuldigte noch nicht über einen Verteidiger verfügt. Da der Beschuldigte selbst keine *security clearance* erhalten wird, können ihm gegenüber die Dokumente nicht zugänglich gemacht werden. Auf diese Situation reagieren die Gerichte durch die Bestellung eines sogenannten *standby defense counsel*. Dieser vertritt die Interessen des Beschuldigten und erhält zu diesem Zweck Zugang zu den Materialien.[795]

b) Während der Hauptverhandlung

Ein auf nationale Sicherheitsinteressen gestützter Ausschluss des Angeklagten während der Hauptverhandlung wurde von den Gerichten bisher abgelehnt.[796] Der Angeklagte kann lediglich nach den allgemeinen Regeln des Zeugenschutzes von bestimmten Vernehmungen ausgeschlossen werden.[797] Abseits dieser Sonderregelungen ist er nach der *Rule* 43 FRCrimP während des gesamten Verfahrens zur Anwesenheit berechtigt.[798] Ein Ausschluss des Angeklagten von weiten Teilen der Hauptverhandlung ist unzulässig und würde nicht zuletzt die Grundprinzipien eines adversatorischen Verfahrens erheblich in Mitleidenschaft ziehen.[799] Allerdings dürfen die faktischen Auswirkungen einer im Vorverfahren erfolgenden *protective order* nicht unberücksichtigt bleiben. Obwohl diese bereits im Stadium der Beweisprüfung erfolgt, wird der Angeklagte als Folge des Sprechverbots selbst während der Hauptverhandlung nichts von den im Vorverfahren diskutierten Umstände erfahren.[800] Insofern bleiben ihm zwar bestimmte Aspekte verborgen, sein Informationsstand unterscheidet sich in diesem Fall jedoch nicht von demjenigen der Geschworenen. Da diese letztlich die Entscheidung über die Schuldfrage fällen, ist der Wissensvorsprung der Anklage weniger bedenklich als man zunächst annehmen würde. Eine zwischen dem Angeklagten und den Geschworenen differenzierende Offenlegung ist nach dem CIPA nicht möglich.[801]

---

795 Vgl. *United States v. Moussaoui*, 333 F.3d 509, 513 (4th Cir. 2003); bestätigt in *United States v. Moussaoui*, 591 F.3d 263, 294 (4th Cir. 2010); *Turner/Schulhofer,* S. 26. Kritisch dazu *Turner/Schulhofer,* S. 26.

796 Vgl. *Chesney,* in: Commission of Inquiry, S. 113; *Turner/Schulhofer,* S. 32.

797 Vgl. zum Schutz von Kindern 18 U.S.C. § 3509 sowie allgemein 18 U.S.C. Ch. 224 mit dem Titel "Protection of Witnesses"; vgl. *Thaman,* in: Perron, S. 515f.

798 Vgl. Rule 43(a)(2): "the defendant must be present at every trial stage".

799 Allgemein dazu *Coy v. Iowa*, 487 U.S. 1012, 1017 (1988); *Kentucky v. Stincer*, 482 U.S. 730, 736, 740 (1987); vgl. zudem *Turner/Schulhofer,* S. 32.

800 So wohl *Turner/Schulhofer,* S. 21.

801 Vgl. *Turner/Schulhofer,* S. 20.

c) Zwischenergebnis

Der dem Verteidiger vorbehaltene Zugang zu geheimhaltungsbedürftigen Erkenntnissen kann nur im Vorverfahren Anwendung finden. Der dortige Ausschluss des Angeklagten kann in bestimmten Fällen faktisch bis in die Hauptverhandlung fortwirken. Ein körperlicher Ausschluss des Angeklagten während verfahrensrelevanter Umstände ist demgegenüber nicht zulässig.

4. Strategie des Geschworenenausschlusses

a) Vor der Hauptverhandlung

Der vor der Hauptverhandlung auf nationale Sicherheitsinteressen gestützte Ausschluss der Geschworenen kommt nicht in Betracht. Die dem *trial* vorgeschalteten Verfahrensstadien erfolgen von vorneherein ohne Beteiligung dieses Laiengremiums. Dies gilt sowohl für die *preliminary hearings* als auch die richterliche Beurteilung der *pretrial motions.* Die Einbeziehung der für die Anklageprüfung zuständigen *grand jury* ändert an dieser Einschätzung nichts, da deren Mitglieder nicht mit den Geschworenen der späteren Hauptverhandlung identisch sind.[802] Die Auswahl der über die Schuldfrage urteilenden Geschworenen erfolgt erst kurz vor der Durchführung der Hauptverhandlung, sodass eine vorherige Teilnahme bereits denknotwendig ausscheidet.[803] Sie sollen ihre Überzeugung unbeeinflusst aus der Hauptverhandlung schöpfen können. Eine vorherige Beteiligung würde zu einer ungewünschten Beeinflussung führen. Zwar können bereits im Vorfeld der Hauptverhandlung bestimmte Mechanismen ablaufen, die den Umfang der den Geschworenen später zur Verfügung stehenden Informationen aus nationalen Sicherheitsinteressen begrenzen, sie entfalten ihre Wirkung jedoch erst im Rahmen der Hauptverhandlung und werden daher im nächsten Abschnitt untersucht.

b) Während der Hauptverhandlung

Eine auf nationale Sicherheitsinteressen gestützte Geheimhaltung gegenüber den Geschworenen während der Hauptverhandlung ist sowohl als mittelbare Folge des § 6 CIPA als auch über die Vorschrift des § 8 CIPA denkbar. Maßgebliches Unterscheidungskriterium ist der Zeitpunkt, in dem die Geheimhaltungsbedürftigkeit bekannt wird. Dieser ist nach der Grundkonzeption des CIPA auf den frühestmöglichen Zeitpunkt festgelegt, wodurch sowohl der Schutz der geheimhaltungsbedürftigen Information gewährleistet wird als auch Überraschungsmomente im

---

802 Vgl. *Trüg,* S. 50.

803 Vgl. *Thompson/Nored/Worrall/Hemmens,* S. 53; *Trüg,* S. 51.

Prozess verhindert werden sollen.[804] Der CIPA verpflichtet die Beteiligten daher, die beabsichtigte Nutzung von *classified information* vorab anzuzeigen. Besteht die Nutzungsabsicht aufseiten des Angeklagten, ist dieser verpflichtet sowohl dem Gericht als auch der Regierung seine Nutzungsabsicht spätestens 30 Tage vor Durchführung des Prozesses mitzuteilen.[805] Diese Mitteilung muss eine kurze Beschreibung der betreffenden Information enthalten, welche der Exekutive eine Einschätzung der bei einer Offenlegung drohenden Risiken ermöglichen soll.[806] Eine bloß grobe Beschreibung ist hierfür nicht ausreichend. Im Anwendungsbereich des CIPA werden damit die dem Angeklagten gegenüber der Regierung obliegenden Offenlegungspflichten erweitert. Kommt der Angeklagte dieser Mitteilungspflicht nicht nach, kann das Gericht diese Missachtung durch Ausschluss des Beweismittels oder der Verteidigungseinrede sanktionieren.[807] Besteht die Nutzungsabsicht aufseiten der Regierung, ist diese ebenfalls zu einer entsprechenden Mitteilung verpflichtet.[808] Sie muss beim Gericht einen Antrag auf Durchführung eines Verfahrens nach § 6 CIPA stellen und dies dem Angeklagten unter Nennung der zu überprüfenden Information mitteilen.[809] Im Regelfall wird die Nutzung von *classified information* damit bereits im Vorfeld bekannt. Diese Konstellation wird von § 6 CIPA abgedeckt, während die Fälle einer erst später bekannt werdenden Geheimhaltungsbedürftigkeit durch § 8 CIPA behandelt werden.

aa) Verfahren des § 6 CIPA

Auf der Grundlage des § 6 CIPA werden vor der eigentlichen Hauptverhandlung die Verwertbarkeit, die Relevanz und die Zulässigkeit der geheimhaltungsbedürftigen Information als Beweismittel geprüft.[810] Die Teilnahme an dieser Prüfung wird auf Antrag des *Attorney General* auf die Verteidigung und die Staatsanwaltschaft begrenzt, wenn dieser bei einem öffentlichen Verfahren die Offenlegung geheimhaltungsbedürftiger Informationen befürchtet.[811] Zwar greift das Verfahren

---

[804] Vgl. *Thaman,* in: Perron, S. 530. Vertiefend zu Zeitpunkt und Zweck der Mitteilungspflicht *Kris/Wilson,* § 27:2, S. 172f.

[805] 18 U.S.C. app. § 5(a).

[806] 18 U.S.C. app. § 5(a): "Such notice shall include a brief description of the classified information." Vgl. *Kris/Wilson,* § 27:2, S. 172.

[807] 18 U.S.C. app. § 5(b) sowie *Thaman,* in: Perron, S. 530.

[808] 18 U.S.C. app. § 6(b); vgl. zudem *Kris/Wilson,* § 27:5, S. 184.

[809] 18 U.S.C. app. § 6(a), § 6(b)(1); vgl. *Kris/Wilson,* § 27:5, S. 184f.

[810] 18 U.S.C. app. § 6(a): "request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding". Vgl. *Kris/Wilson,* § 27:5, S. 182f.

[811] 18 U.S.C. app. § 6(a): "Any hearing held […] shall be held in camera if the *Attorney General* certifies to the court in such petition that a public proceeding may result in the disclosure of classified information."

nach § 6 CIPA bereits im Vorfeld einer Hauptverhandlung, da den Geschworenen allerdings nur die nach § 6 CIPA zugelassenen Beweismittel vorgelegt werden können, sind diese vorgeschalteten Prüfungsvorgänge für den Wissensstand im Rahmen des Hauptverfahrens von Bedeutung. Bejaht das Gericht in dieser Phase die Ersetzbarkeit der Beweismittel, sind die geheimhaltungsbedürftigen Informationen im späteren Hauptverfahren weder den Geschworenen noch der Öffentlichkeit zugänglich.[812] Ein Ausschluss der Geschworenen von bestimmten Wissenselementen ist damit mittelbar über die Regelung des § 6 CIPA denkbar.

Das Verfahren nach § 6 CIPA kennt grundsätzlich zwei Anwendungsfälle. Der erste Fall betrifft die besagte *graymail*-Situation.[813] In dieser möchte der Angeklagte geheimhaltungsbedürftige Informationen zu seinen Gunsten einführen beziehungsweise durch Androhung der Offenlegung die Regierung zu einer Verfahrenseinstellung bewegen. In einer solchen Konstellation wird die Exekutive versuchen eine Offenlegung der Erkenntnisse im Prozess zu verhindern und die Zulässigkeit beziehungsweise Ersetzbarkeit des Beweismittels durch das Gericht nach § 6 CIPA überprüfen zu lassen.[814] Der zweite Fall besteht bei einer Nutzungsabsicht der Regierung, wenn diese die geheimhaltungsbedürftigen Informationen zur Überführung des Täters zwar nutzen, aber nicht vollständig offenlegen möchte.[815] In beiden Anwendungsfällen hat der Angeklagte bereits Zugang zu den geheimhaltungsbedürftigen Informationen. Dieser kann entweder aus einer Offenlegung nach § 4 CIPA oder einer bereits vorher bestehenden Zugangsmöglichkeit stammen.

In materieller Hinsicht nimmt der Richter nach § 6(a), (c) CIPA erneut eine zweistufige Prüfung vor. Auf einer ersten Stufe werden die Verwertbarkeit, die Relevanz und die Zulässigkeit der geheimhaltungsbedürftigen Information als Beweismittel geprüft. Fällt diese Entscheidung positiv aus, wird auf einer zweiten Stufe die Ersetzbarkeit des Beweismittels durch ein Beweissurrogat erörtert. Die auf der ersten Stufe erforderliche Relevanz- und Zulässigkeitsprüfung richtet sich theoretisch nach den allgemeinen Regeln.[816] Relevante Beweise sind dementsprechend zuzulassen, sofern keine besondere Ausnahme eingreift.[817] Nach der *Rule* 401 FRE ist ein Beweismittel relevant, wenn es die Chancen verbessert, eine Tatsache zumindest teilweise zu belegen beziehungsweise zu widerlegen und die

---

[812] Ein *ex parte*-Verfahren ist im Rahmen des 18 U.S.C. app. § 6 grundsätzlich nicht zulässig, da beide Parteien zur Relevanz des Beweismittels i.S.d. Rule 401 FRE gehört werden sollen. Lediglich die eidesstattliche Versicherung nach § 6(c)(2) kann *ex parte* untersucht werden. In diesem Fall wäre die Vorschrift der dritten Geheimhaltungsstrategie zuzuordnen.

[813] Vgl. *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1067.

[814] Vgl. *Kris/Wilson,* § 27:2, S. 172.

[815] Vgl. *Kris/Wilson,* § 27:7, S. 195.

[816] Es gelten folglich die FRE 401ff und 802ff, vgl. auch *Kris/Wilson,* § 27:6, S. 187ff.

[817] Eine Ausnahme wäre nach FRE 403 bei einer unfairen Benachteiligung oder nach FRE 802 bei einem Hörensagenbeweis denkbar.

Erkenntnis für den Ausgang des Rechtsstreits von Belang ist.[818] Obwohl diese Vorgaben grundsätzlich auch im Rahmen des CIPA zur Anwendung kommen sollen, hat sich in der Rechtsprechung ein abweichender Prüfungsmaßstab durchgesetzt.[819] In diesem wird die Relevanz anhand einer Abwägung zwischen den Verteidigungs- und Geheimhaltungsinteressen bestimmt.[820] Entgegen der sonst üblichen Relevanzprüfung muss der Angeklagte nachweisen, dass das Beweismittel für einen fairen Strafprozess selbst unter Einbeziehung der Geheimhaltungsinteressen unerlässlich ist.[821] Der Angeklagte muss dementsprechend belegen können, dass die Informationen seine Argumentation tatsächlich stützen.[822] Die von der klassischen Relevanzprüfung abweichende Abwägungslösung der Rechtsprechungspraxis erhöht damit die an eine Zulassung geheimhaltungsbedürftiger Informationen anzulegenden Standards.[823] Als Konsequenz wurde die Notwendigkeit der Informationen für die Verteidigung von den Gerichten in den meisten Fällen abgelehnt.[824] Verneint das Gericht in diesem Sinne das Bestehen einer Offenlegungspflicht, kann der Angeklagte jedoch jederzeit die Nachprüfung der Entscheidung veranlassen.[825]

Bejaht das Gericht umgekehrt die Relevanz und Zulässigkeit des Beweismittels, wird auf einer zweiten Stufe die Ersetzbarkeit durch Beweissurrogate geprüft. Diese müssen dem Angeklagten im Grundsatz die gleichen Verteidigungsmöglichkeiten bieten, die bei der Offenlegung der unmittelbaren Beweismittel bestanden hätten.[826] Dieser Nachweis muss durch die Regierung erbracht werden.[827] Erforderlich und ausreichend ist die Vergleichbarkeit der Verteidigungsmöglichkeiten, eine absolute Identität ist nicht notwendig.[828] In Bezug auf die tauglichen Beweissurrogate sieht das Gesetz zwei Möglichkeiten vor. Danach können die geheimhaltungs-

---

[818] FRE 401: "Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." Die Beweislast liegt beim Angeklagten, vgl. *Kris/Wilson,* § 27:6, S. 186f.

[819] Die Rechtslage ist insgesamt umstritten. Zum Teil sollen die Geheimhaltungsinteressen generell überwiegen, vgl. *United States v. Nixon*, 418 U.S. 683, 706 (S. Ct. 1974). Vgl. demgegenüber *United States v. Coplon*, 185 F.2d 629, 638 (2d Cir. 1950). Vertiefend *Stacy,* U. Colo. L. Rev. (58) 1987, S. 180ff, S. 187 Fn. 19.

[820] Zur ü.A. vgl. *Kris/Wilson,* § 27:6, S. 188f; *Stacy,* U. Colo. L. Rev. (58) 1987, S. 182.

[821] Vgl. *Kris/Wilson,* § 27:6, S. 189. Dieser Test gilt auch im Rahmen des § 4 CIPA.

[822] Vgl. *Shea,* Am. Crim. L. Rev. (27) 1990, S. 671.

[823] Vgl. *Kris/Wilson,* § 27:6, S. 188.

[824] Vgl. *Kris/Wilson,* § 27:6, S. 191.

[825] Siehe § 6(d) CIPA; vgl. *Kris/Wilson,* § 27:6, S. 187.

[826] Vgl. *Kris/Wilson,* § 25:3, S. 129; *Thaman,* in: Perron, S. 527.

[827] Siehe *United States v. Fernandez*, 913 F. 2d, 162 (4th 1990): "we think the burden must be on the government to delineate the substitutions' precise scope before the trial court"; vgl. hierzu ebenfalls *Kris/Wilson,* § 27:7, S. 193.

[828] Vgl. *Kris/Wilson,* § 27:7, S. 193.

bedürftigen Informationen entweder durch eine Zusammenfassung der relevanten Informationen oder durch das schriftliche Zugeständnis der behaupteten Tatsachen ersetzt werden.[829] In der letzten Konstellation werden die von der Verteidigung aufgestellten Behauptungen als wahr unterstellt.[830] Bejaht das Gericht in diesem Zusammenhang sowohl die Geheimhaltungsbedürftigkeit als auch die Ersetzbarkeit, kann anstelle der geheimhaltungsbedürftigen Informationen eines der besagten Surrogate eingeführt werden. Die geheimhaltungsbedürftige Information selbst wird weder den Geschworenen noch der Öffentlichkeit zugänglich gemacht.

Verneint das Gericht die Ersetzbarkeit, sind die fraglichen Informationen grundsätzlich offenzulegen. Die Entscheidung, ob es tatsächlich zu einer Offenlegung kommt, obliegt jedoch weiterhin der Exekutive.[831] Wie bereits in den vorherigen Konstellationen kann der *Attorney General* durch eine eidesstattliche Erklärung der Offenlegung widersprechen.[832] Die damit verbundene Nichtoffenlegung ist jedoch an einschneidende Sanktionen geknüpft, deren konkrete Ausgestaltung von der Bedeutung der Information für das konkrete Strafverfahren bestimmt wird. Betreffen die Informationen wesentliche Fragen der Schuld beziehungsweise Unschuld, führt die endgültige Verweigerung der Regierung zur Einstellung des Strafverfahrens.[833] Von dieser Regel wird eine Ausnahme gemacht, wenn die Regierung darlegen kann, dass eine Verfahrenseinstellung dem Gerechtigkeitsempfinden widersprechen würde. Für diesen Fall kann das Gericht andere Sanktionen aussprechen. Mögliche Alternativen sind die bloß teilweise Verfahrenseinstellung, das Zugeständnis der unterstellten Tatsachen oder der Ausschluss bestimmter Zeugenaussagen.[834] Die verschiedenen Sanktionen dienen hierbei nicht der Bestrafung der Regierung, sondern sollen die durch die Geheimhaltung beeinträchtigte Verfahrensfairness ausgleichen und die Integrität des Verfahrens sicherstellen.[835] Entspre-

---

[829] Siehe § 6(c) CIPA: "in lieu of the disclosure […], the court order (A) the substitution for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove; or (B) the substitution for such classified information of a summary of the specific classified information".

[830] Vgl. *Thaman,* in: Perron, S. 526.

[831] Vgl. *Kris/Wilson,* § 27:8, S. 196; *Yaroshefsky,* Hofstra L. Rev. (34) 2006, S. 1069.

[832] 18 U.S.C. app. § 6(e)(1): "Whenever the court denies a motion by the United States that it issue an order under subsection (c) and the United States files with the court an affidavit of the *Attorney General* objecting to disclosure of the classified information at issue, the court shall order that the defendant not disclose or cause the disclosure of such information." Eine gerichtliche Überprüfung dieser Erklärung ist nicht vorgesehen, vgl. *Kris/Wilson,* § 27:8, S. 197.

[833] 18 U.S.C. app. § 6(e)(2): "Whenever a defendant is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment or information; except that, when the court determines that the interests of justice would not be served by dismissal of the indictment or information, the court shall order such other action"

[834] 18 U.S.C. app. § 6(e)(2)(A)–(C), vgl. *Thaman,* in: Perron, S. 526.

[835] Vgl. *Turner/Schulhofer,* S. 20.

chend dieser Zwecksetzung wird das Gericht die Sanktionen auf das für eine Kompensation notwendige Maß festlegen.[836] Ebenso wie im Anwendungsbereich des § 4 CIPA kann die Regierung die gerichtliche Entscheidung einer Zwischenprüfung nach § 7 CIPA unterziehen.

bb) Verfahren des § 8 CIPA

Daneben kommt eine Geheimhaltung auf der Grundlage des § 8 CIPA in Betracht. Die Vorschrift greift bei einem Sachverhalt, bei dem die Geheimhaltungsbedürftigkeit der einzuführenden Information erst später bekannt wird und daher eine Vorabprüfung nach den §§ 4, 6 CIPA nicht durchgeführt werden konnte.[837] Um dennoch eine Offenlegung sensibler Informationen verhindern zu können, gestattet die Vorschrift des § 8 CIPA den Erlass von Schutzmaßnahmen während der Hauptverhandlung. Diese können verschiedene Schutzvorkehrungen beinhalten. Als eine Möglichkeit können beispielsweise geheimhaltungsbedürftige Abschnitte eines Dokuments für die Zwecke der Hauptverhandlung zeitweise entnommen werden, sofern nicht eine vollständige Offenlegung aus Gründen der Verfahrensfairness geboten ist.[838] Schließlich kann das Gericht auf Verlangen der Regierung in eine Zeugenvernehmung eingreifen, wenn durch die Befragung des Zeugen die Offenlegung sensibler Informationen droht.[839] Hierzu wird die Zulässigkeit der Aussage zusammen mit der möglichen Schutzmaßnahme *in camera* geprüft.[840] Das Gericht kann in diesem Fall vom Angeklagten verlangen, dass er seine an den Zeugen zu stellenden Fragen vorab zur Verfügung stellt und präzisiert. Durch diese Präzisierung wird die Regierung in die Lage versetzt, eine taugliche, den Geheimhaltungsbedürfnissen Rechnung tragende Antwort zu verfassen.[841] Um eine unbeabsichtigte Offenlegung geheimhaltungsbedürftiger Informationen zu verhindern, wird bei diesem Vorgang letztlich die ursprünglich unkontrollierbare Zeugenaussage durch eine vorformulierte Aussage ersetzt. Im Ausnahmefall können den Geschworenen damit auch im Stadium der Hauptverhandlung noch Erkenntnisse vorenthalten werden.

---

[836] Vgl. *United States v. Fernandez*, 913 F.2d 148, 163 (4th 1990); *Kris/Wilson,* § 27:8, S. 197.

[837] In diesem Fall läuft die nach § 5 CIPA bestehende Mitteilungspflicht ins Leere, vgl. das Criminal Resource Manual 2054 des Justizministeriums unter Punkt III.B.; zu finden unter www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm02054.htm [Stand: 1.5.2012].

[838] Vgl. § 8(b) CIPA als Präzisierung der FRE 106; vgl. *Kris/Wilson,* § 27:11, S. 202ff.

[839] § 8(c) CIPA.

[840] Vgl. hierzu *Kris/Wilson,* § 27:11, S. 204.

[841] Vgl. *Turner/Schulhofer,* S. 21.

5. Strategie des Öffentlichkeitsausschlusses

Die fünfte Konstellation betrifft den Ausschluss der Öffentlichkeit.[842] Der Grundsatz der Öffentlichkeit wird durch den ersten und sechsten Verfassungszusatz garantiert und soll die Fairness, Akzeptanz und die Kontrolle gerichtlicher Entscheidungen gewährleisten.[843] Ein Ausschluss der Öffentlichkeit auf der Grundlage des CIPA ist nicht vorgesehen.[844] Verfahren vor den Bundesgerichten sind damit grundsätzlich öffentlich.[845]

In bestimmten Ausnahmefällen haben die Gerichte allerdings Abweichungen vom Grundsatz der Öffentlichkeit zugelassen.[846] Die Voraussetzungen der richterlichen Ausschlussregelung sind sehr allgemein gehalten. Grundbedingung ist zunächst das Vorliegen eines legitimen Geheimhaltungszwecks. Nach Ansicht der Richter ist ein Ausschluss der Öffentlichkeit nur zum Schutz hochrangiger Werte und Interessen zulässig. Darüber hinaus müssen die Voraussetzungen des Verhältnismäßigkeits- und Subsidiaritätsgrundsatzes beachtet werden. Ein Ausschluss der Öffentlichkeit ist dementsprechend nur beim Fehlen alternativer Schutzvorkehrungen und in wenigen Ausnahmefällen möglich.[847] Als abschließendes Korrektiv dürfen die Verteidigungschancen nicht hinter denen eines öffentlichen Strafverfahrens zurückbleiben.

Sind die genannten Voraussetzungen erfüllt, kann das Gericht verschiedene Schutzvorkehrungen treffen, die sich auf die Teilhabe der Öffentlichkeit (am Wissen) auswirken können. Der konkrete Umfang des Öffentlichkeitsausschlusses bestimmt sich in Abhängigkeit von der Bedeutung des Beweismittels, den sonstigen Erkenntnismöglichkeiten der Öffentlichkeit und dem staatlichen Interessen an einer Geheimhaltung.[848] Neben dem vollständigen Ausschluss der Öffentlichkeit von bestimmten Verfahrensabschnitten kommt beispielsweise die unter einem Pseudonym erfolgende, anonyme Zeugenaussage in Betracht.[849] Daneben hat sich die sogenannte *silent witness rule* etabliert.[850] Nach dieser Rechtsfigur erfolgt die

---

[842] Vgl. zum Ausschluss der Öffentlichkeit *Turner/Schulhofer,* S. 29ff.

[843] Vgl. *Scheb/Scheb II,* S. 364; *Turner/Schulhofer,* S. 14.

[844] Vgl. *Turner/Schulhofer,* S. 29.

[845] Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 44.

[846] Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 44 Fn. 127; *Zabel/Benjamin,* S. 86 m.w.N.

[847] Siehe *Press-Enterprise Co. v. Superior Court*, 464 U.S. 501, 510 (1984): "The presumption of openness in a criminal trial may be overcome only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest."

[848] Vgl. *Turner/Schulhofer,* S. 30.

[849] Vgl. *Chesney,* in: Commission of Inquiry, S. 49, 112; *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 44; *Zabel/Benjamin,* S. 101f, jeweils m.w.N.

[850] Vgl. *United States v. Abu Ali*, 528 F.3d 210 (4th Cir. 2008), cert. denied, *United States v. Abu Ali*, 129 S. Ct. 1312 (2009); *United States v. Zettl*, 835 F.2d 1059, 1063 (4th

Zeugenaussage unter Verwendung eines vorab entwickelten Codes, der die geheimhaltungsbedürftigen Aspekte der Information beschreibt und durch unverfängliche Begriffe ersetzt. Ein Zeuge tritt in einem Verfahren beispielsweise nicht unter seinem wirklichen Namen, sondern unter der Bezeichnung „Zeuge X" auf.[851] Die Aufschlüsselung der verwendeten Abkürzungen ist nur den Verfahrensbeteiligten, dem Gericht und den Geschworenen bekannt. Die Öffentlichkeit ist nicht in die Codierung involviert, sodass bestimmte Aspekte eines Beweismittels nicht öffentlich werden. Erwähnenswert ist weiterhin, dass eine geheimhaltungsbedürftige Information durch eine Offenlegung gegenüber dem Angeklagten ihren Schutz nicht auch automatisch gegenüber der Öffentlichkeit verliert.[852] Die strafprozessuale Nutzung führt nicht zu einer Aufhebung der Geheimhaltungsstufe.[853] Das Gericht kann dem Angeklagten daher mittels einer Schutzanordnung die weitere Offenlegung der Informationen verbieten.[854]

Erleichterte Voraussetzungen eines Öffentlichkeitsausschlusses gelten in einem Verfahren vor einer Militärkommission. Dort ist der Militärrichter befugt, die Öffentlichkeit ganz oder teilweise auszuschließen, wenn dies zum Schutz sicherheitsrelevanter Informationen oder der körperlichen Unversehrtheit einer Person erforderlich ist.[855] Schutzwürdig ist die Information, wenn die Offenlegung vernünftigerweise die nationale Sicherheit, Informationsquellen oder -methoden sowie Aktivitäten der Geheimdienste und Strafverfolgungsbehörden gefährden kann. Zusätzlich zu den bereits genannten Ausschlussmöglichkeiten kann in einer Militärkommission eine Zeugenaussage mittels Funkübertragung mit einer zeitlichen Verzögerung von 45 Sekunden übertragen werden. Diese Zeitspanne ermöglicht einen rechtzeitigen Abbruch der Zeugenaussage, wenn die Offenlegung geheimhaltungsbedürftiger Informationen droht.[856] Eine vergleichbare Möglichkeit existiert in der zivilen Strafgerichtsbarkeit bislang nicht.

Im Ergebnis können bestimmte Beweismittel oder Verfahrensabschnitte zum Schutz nationaler Sicherheitsinteressen gegenüber der Öffentlichkeit geheim blei-

---

Cir. 1987) cert. denied *United States v. Zettl*, 494 U.S. 1980 (1990); *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 45; *Turner/Schulhofer,* S. 29; *Zabel/Benjamin,* S. 102.

851 Vgl. *Zabel/Benjamin,* S. 102.

852 Vgl. *Chesney,* in: Commission of Inquiry, S. 111.

853 Siehe § 8(a) CIPA: "may be admitted into evidence without change in their classification status." Vgl. *Kris/Wilson,* § 25:2, S. 123.

854 Siehe § 3 CIPA: "Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States."

855 So 10 U.S.C. § 949d(c)(2): "The military judge may close to the public all or a portion of the proceedings under paragraph (1) only upon making a specific finding that such closure is necessary to (A) protect information the disclosure of which could reasonably be expected to cause damage to the national security, including intelligence or law enforcement sources, methods, or activities; or (B) ensure the physical safety of individuals."

856 Vgl. *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 45 Fn. 129.

ben. In Militärkommissionen ist der Öffentlichkeitausschluss zudem unter erleichterteren Bedingungen möglich als in der klassischen Bundesgerichtsbarkeit.[857]

V. Zusammenfassung zur amerikanischen Rechtslage

Als Vergleichsäquivalent diente der Untersuchung das FBI. Es ist der Hauptproduzent von Geheimdienstinformationen in den USA und verfügt nach dem FISA über umfassende Ermittlungsbefugnisse.

An seinem Beispiel konnte der Einfluss der Sicherheitsarchitektur auf die Besonderheiten geheimdienstlicher Ermittlungen und die strafprozessuale Nutzung von Geheimdienstinformationen nachgewiesen werden. Die verfassungsrechtlich geprägten Strukturen des amerikanischen Sicherheitswesens wirken sich unmittelbar auf die Gestaltung des Geheimdienst- und Strafverfolgungssektors aus. Entsprechend den Anforderungen des vierten Verfassungszusatzes wird zwischen *domestic intelligence investigations* und *foreign intelligence investigations* differenziert. Diese Grenzziehung ist auf die erhöhten verfassungsrechtlichen Schutz standards für rein inländische Beobachtungssubjekte zurückzuführen. Sie bedingt, dass formal weiterhin zwischen rein inländischen Sachverhalten (DII) und solchen mit Auslandsbezug (FII) unterschieden wird. Der Bereich der DII folgt dabei weitgehend den strafrechtlichen Regeln, wohingegen sich die FII nach den Vorgaben des FISA richten. Die Differenzierung zwischen Straf- und Geheimdienstrecht ist damit vor allem hinsichtlich der Anwendung des FISA von Bedeutung. Sie wirkt sich auf die jeweils geltenden Ermittlungsschwellen, Erhebungsvoraussetzungen und Kontrollinstanzen aus. Insbesondere der FISA stellt in den meisten Fällen geringere Anforderungen. Seit den Reformen aus dem Jahr 2001 und der damit einhergehenden Umgestaltung der Sicherheitsarchitektur verliert diese Aufteilung allerdings an Bedeutung. Durch die Öffnung des FISA wurden die meisten geheimdienstlichen Befugnisse auch anderen Ermittlungszwecken zugänglich gemacht.

Ebenfalls von Bedeutung ist die Zwitterstellung des FBI, welches faktisch sowohl geheimdienstliche als auch polizeiliche Aufgaben wahrnimmt. Diese Behördenidentität zusammen mit den Änderungen des FISA bedingen, dass das amerikanische Recht der Nutzung geheimdienstlicher Erkenntnisse grundsätzlich offen gegenübersteht. Die Übermittlung von Geheimdienstinformationen zu Zwecken der

---

[857] Noch weitere Einschränkungen sind im Rahmen der präventiven Verwaltungshaft möglich; vgl. insgesamt *Kris,* J. Nat'l Sec. L. & Pol'y (5) 2011, S. 45f.

Strafverfolgung wird umfassend gestattet. Selbst die Übermittlung von FISA-Erkenntnissen unterliegt keinen nennenswerten inhaltlichen Schranken. Lediglich in Bezug auf Informationen über *U.S. Persons* finden sich vereinzelte Einschränkungen. Die Verwertbarkeit von Geheimdienstinformationen wird ebenfalls kaum problematisiert. Insbesondere im Bereich der inlandsbezogenen Aufklärung müssen aufgrund der identischen Erhebungsstandards keine beweisrechtlichen Sonderregeln beachtet werden. Seit der Öffnung des FISA im Jahr 2001 sind Erkenntnisse der *foreign intelligence investigations* in den meisten Fällen unabhängig von der ursprünglichen Zielsetzung verwertbar.

Darüber hinaus konnte die Untersuchung die Auswirkungen nationaler Sicherheitsinteressen auf die Nutzung und Offenlegung von Geheimdienstinformationen in einem Strafverfahren verdeutlichen. Im amerikanischen Strafverfahren wird der Schutz geheimhaltungsbedürftiger Informationen vor allem durch die Regelungen des CIPA und des FISA ermöglicht. Während der FISA nur auf FISA-Vorgänge anwendbar ist, kommt der CIPA allgemein bei *classified information* und damit in der Mehrzahl der Fälle zur Anwendung. Beide Regelwerke enthalten verschiedene Kontroll- und Surrogationsmechanismen, die einen sicheren Umgang mit geheimhaltungsbedürftigen Vorgängen und Informationen sicherstellen sollen. Die wesentlichen Geheimhaltungsentscheidungen werden vor der Hauptverhandlung in einem Überprüfungsverfahren getroffen, dass der Richter allein durchführt. Bejaht er sowohl die Geheimhaltungsbedürftigkeit als auch die Relevanz der Information, wird eine Ersetzung der fraglichen Erkenntnisse durch gesetzlich normierte Beweissurrogate gestattet. Bei einer Missachtung der gerichtlich festgestellten Offenlegungspflicht greifen Sanktionsmechanismen. Diese können bis zu einer Verfahrenseinstellung reichen. Die im amerikanischen Recht vorgesehenen Kontroll- und Surrogationsmodelle sollen die Offenlegung irrelevanter, aber schutzwürdiger Informationen verhindern sowie eine sichere Nutzung notwendiger Erkenntnisse gewährleisten.

Der strafrichterlichen Kontrolle kommt damit in beiden Problemkreisen eine herausragende Stellung zu. Über die *warrant*-Vorgaben des vierten Verfassungszusatzes einerseits sowie über die Regelwerke des FISA und des CIPA andererseits werden dem Richter wichtige Entscheidungs- und Kontrollmöglichkeiten eingeräumt. Sobald geheimdienstliche Erkenntnisse die Schwelle zum Strafverfahren überschreiten, soll damit vor allem der Strafrichter die Fairness des späteren Strafverfahrens sicherstellen.

Teil 4

Vergleichende Gegenüberstellung

Die strafprozessuale Nutzung von Geheimdienstinformationen wirft im deutschen und amerikanischen Recht zahlreiche Fragen auf. Die wechselseitigen Spannungen zwischen den staatlichen Strafverfolgungs- und Sicherheitsinteressen sowie den Persönlichkeits- und Freiheitsinteressen des Einzelnen versuchen die nationalen Lösungsmodelle auf unterschiedliche Art und Weise aufzulösen. Die nachfolgenden Ausführungen orientieren sich an der Struktur der Landesberichte und stellen die jeweils erzielten Erkenntnisse vergleichend gegenüber.

I. Grundlagen in geheimdienstrelevanten Strafverfahren

Über die klassischen Unterschiede des deutschen und amerikanischen Strafverfahrensrechts hinaus konnten für die vorliegende Fragestellung spezifische Besonderheiten festgestellt werden. Diese betreffen zunächst die in geheimdienstrelevanten Strafverfahren anwendbaren Zuständigkeitsregeln und Sonderinstitute.

Geheimdienstrelevante Strafverfahren werden sowohl im deutschen als auch im amerikanischen Recht vor Gerichten auf Bundesebene geführt. Durch diese Zuständigkeitsverteilung werden die besonderen Anforderungen solcher Strafverfahren deutlich. Diese bundesgerichtliche Zuordnung entspricht weder im deutschen noch im amerikanischen Recht der Regelzuständigkeit. Beide Rechtsordnungen folgen vielmehr einem föderalen Ordnungsprinzip, welches die Gerichtshoheit zunächst den Einzelstaaten beziehungsweise den Bundesländern überträgt. Um dennoch eine effektive, zentrale und überregionale Strafverfolgung zu gewährleisten, werden besonders gravierende Fälle der Gerichtshoheit des Bundes übertragen. Zwar wurde in Deutschland die ursprünglich dem BGH zugewiesene erst- und letztinstanzliche Zuständigkeit durch ein mehrstufiges Verfahren ersetzt und die Oberlandesgerichte als erste Instanz vorgeschaltet, jedoch erfolgte die Einbindung der Oberlandesgerichte im Wege der Organleihe, sodass sie formal Bundesgerichtsbarkeit ausüben.[1] Die bei der Nutzung von Geheimdienstinformationen regelmäßig bestehende gesamtstaatliche beziehungsweise staatsschutzgefährdende Relevanz

---

[1] Vgl. Gesetz vom 8.9.1969, BGBl. I, 1969, S. 1582, sowie S. 1236; *Welp,* NStZ 2002, S. 3.

führt damit sowohl im deutschen als auch im amerikanischen Recht zur Annahme einer bundesgerichtlichen (Sonder-)Zuständigkeit.

Über diese Gemeinsamkeit hinaus wurde die Kompetenzverteilung im Allgemeinen in beiden Ländern an akute oder permanente Bedrohungslagen angepasst. Diese Veränderungen waren allerdings von unterschiedlicher Intensität. Während in den USA neue gerichtliche Sonderinstitute geschaffen wurden, erfolgte in Deutschland eine Ausweitung bestehender Überwachungsbefugnisse. Im amerikanischen Recht waren die Änderungen damit letztlich gravierender. Als Reaktion auf die Anschläge von 2001 wurde die zivile Strafgerichtsbarkeit um die sogenannten *Military Commissions* ergänzt. Diese vom deutschen System abweichende Konzeption beruht zu einem erheblichen Teil auf den Besonderheiten der amerikanischen Sicherheitsarchitektur. Diese eröffnet dem Präsidenten durch die verfassungsrechtlich garantierten *war powers* erhebliche Handlungsspielräume, die vor dem Hintergrund der politisch geprägten Kriegsrhetorik umfassend genutzt wurden. Die bis zu den Änderungen des MCA 2009 zum Teil gravierenden Unterschiede wurden zwar vereinzelt abgemildert, dennoch weichen sowohl der Fokus als auch die anwendbaren Beweis- und Verfahrensregeln weiterhin von der zivilen Strafgerichtsbarkeit im amerikanischen und vor allem im deutschen Strafverfahrenssystem ab.

In Deutschland kam es infolge akuter Bedrohungslagen ebenfalls zu Veränderungen im Zuständigkeitsgefüge. Der amerikanische Ansatz einer zusätzlichen Sondergerichtsbarkeit mit unterschiedlichen Beweis- und Verfahrensstandards ist hier allerdings weiterhin undenkbar. Der deutsche Gesetzgeber steht bereits aus historischen Gründen der Einrichtung von Sondergerichten ablehnend gegenüber. Möglichen Bedrohungslagen wird weniger durch eine Anpassung der strafprozessualen Zuständigkeiten als vielmehr durch einen Ausbau bestehender Ermittlungsbefugnisse Rechnung getragen. Dies zeigt sich etwa an der Ausweitung des geheimdienstlichen Beobachtungsauftrags auf den Bereich der organisierten Kriminalität oder der Ergänzung polizeilicher Ermittlungsbefugnisse um ehemals nachrichtendienstliche Instrumentarien. Anders als in den USA wird der Terrorismus jedoch weiterhin als Kriminalitätsphänomen und nicht als Kriegsakt eingestuft.[2] Aus diesem Grund wird, anders als im amerikanischen Modell, weiterhin ein tatbezogener und kein täter- beziehungsweise statusbezogener Ansatz verfolgt. Aufgrund dieses unterschiedlichen Fokus sind die Spielräume des deutschen Gesetzgebers zugleich viel enger als die im amerikanischen Modell. Die zahlreichen Verfassungsbeschwerden gegen die verschiedenen Sicherheitsreformen verdeutlichen jedoch, dass die Veränderungen zum Zweck der Terrorbekämpfung ebenfalls kritisch gesehen werden.

---

[2] Vgl. *Singer,* in: Jäger/Daun, S. 58.

II. Allgemeine Strukturen des Geheimdienstwesens

Bei einer Betrachtung des deutschen und amerikanischen Geheimdienstwesens konnten in beiden Rechtsordnungen Behörden ausgemacht werden, die Geheimdienstinformationen nach der eingangs gewählten Definition erheben. Diese Einrichtungen weisen verschiedene Gemeinsamkeiten und Unterschiede auf, die nachfolgend im Überblick dargestellt werden. Im Mittelpunkt der Untersuchung stehen die quantitative und organisatorische Gestaltung des jeweiligen Geheimdienstwesens, die damit verbundenen strukturellen Herausforderungen sowie die Regelungsdichte des nationalen Geheimdienstrechts.

A. Quantitative und organisatorische Gestaltung

Die Gestaltung des amerikanischen und deutschen Geheimdienstwesens folgt trotz erheblicher quantitativer Unterschiede in organisatorischer Hinsicht ähnlichen Grundstrukturen. Sowohl der deutsche als auch der weitaus größere amerikanische Geheimdienstsektor differenzieren zwischen der militärischen Aufklärung einerseits und der zivilen Aufklärung andererseits.

In quantitativer Hinsicht ist das amerikanische Geheimdienstwesen insgesamt weitaus breiter aufgestellt als das deutsche. Auffallend ist zunächst die unterschiedliche Anzahl der mit Geheimdienstaufgaben betrauten Einrichtungen. Je nach Zählweise stehen den 17 bis 60 US-Behörden etwa drei bis 19 deutsche Dienste gegenüber.[3] Die amerikanischen Dienste sind zudem finanziell weitaus besser ausgestattet.[4] Ein konkreter Vergleich der Finanzbudgets ist allerdings nur bedingt möglich, da sich die Kosten auf eine Vielzahl unterschiedlicher Strukturen verteilen und nicht sämtliche Kosten veröffentlicht werden. Darüber hinaus wird eine Gegenüberstellung durch die erheblichen ökonomischen und geografischen Größenunterschiede zwischen Deutschland und den USA verzerrt.

Die organisatorische Aufteilung der beiden Geheimdienstsektoren ist wiederum sehr ähnlich. In beiden Rechtsordnungen können die einzelnen Dienste der militärischen und zivilen Aufklärung zugeordnet werden, wobei das militärische Geheimdienstwesen jeweils am stärksten ausgeprägt ist. Zusätzlich wird zwischen den Zuständigkeiten im Inland und Ausland differenziert. Entsprechend dieser groben Einteilung stehen den deutschen Diensten ein oder mehrere funktionale Äquivalente des amerikanischen Geheimdienstwesens gegenüber. Als prominentes Beispiel für diese parallelen Strukturen wird üblicherweise die Auslandsaufklärung heran-

---

[3] Vgl. http://www.intelligence.gov [Stand 1.5.2012]; *Hörauf,* S. 289; *Jäger/Daun,* in: Borchert, S. 61.

[4] Eine Übersicht über die verschiedenen Budgets findet sich bei *Daun,* Auge um Auge, S. 130, 144f.

gezogen. Diese wird in Deutschland primär durch den BND, in den USA durch die CIA wahrgenommen. In dieser Funktion unterstehen beide Dienste direkt der Exekutive.[5] Anders als die CIA nimmt der BND die Auslandsaufklärung allerdings umfassend vor. Er kann zu diesem Zweck sowohl auf Methoden der HUMINT als auch der SIGINT zurückgreifen. Im Vergleich dazu wird die CIA lediglich im Bereich der HUMINT tätig, während die signalerfassende Aufklärung durch militärische Dienste, wie etwa die NSA, erfolgt.[6]

B. Gestaltung der Inlandsaufklärung

Markanter Unterschied beider Systeme ist die unterschiedliche Gestaltung der Inlandsaufklärung. Während im deutschen Recht die Inlandsaufklärung durch speziell dafür geschaffene, eigenständige Behörden erfolgt, überrascht das amerikanische Geheimdienstwesen durch den Verzicht auf einen eigenständigen Inlandsgeheimdienst. In beiden Rechtsordnungen existieren jedoch Strukturen, die in funktionaler Hinsicht Aufgaben der Inlandsaufklärung wahrnehmen. In Deutschland werden insofern die Verfassungsschutzbehörden auf Bundes- und Landesebene tätig. In den USA wird diese Aufgabe demgegenüber durch andere Stellen, wie etwa das FBI oder lokale Sicherheitsbehörden, wahrgenommen. Zwar wird auch im amerikanischen Kontext immer wieder die Errichtung eines solchen Dienstes diskutiert,[7] in der Praxis wurde diese Forderung bislang jedoch nicht umgesetzt.

Die in der Inlandsaufklärung bestehenden Unterschiede sind vor allem auf historische Ereignisse und deren Auswirkung auf die Gestaltung der Sicherheitsarchitektur zurückführbar. Eine erste Ursache liegt in den Grundstrukturen, die bestanden, als jeweils die Errichtung eines Inlandsgeheimdienstes diskutiert wurde. Bei der Errichtung des BfV im Jahr 1950 waren keine konkurrierenden Behördenstrukturen vorhanden, die dem Aufbau eines Inlandsnachrichtendienstwesens entgegengestanden hätten. Im Vergleich dazu fanden sich bei der Strukturierung des amerikanischen Geheimdienstwesens durch den *National Security Act* von 1947 mit dem FBI für das Inland bereits gefestigte Strukturen. Da das FBI heute wie damals an seiner Vormachtstellung festhält, mussten sich die sonstigen geheimdienstlichen Strukturen auf den verbleibenden Bereich der Auslandsaufklärung beschränken.

Eine zweite Ursache bilden politische Ereignisse, welche die Entwicklung des Geheimdienstwesens begleiteten und durch die Gestaltung des nationalen Rechts begünstigt wurden. In den USA kam es in den 1970er Jahren aufgrund einer

---

[5] Vgl. hierzu *Daun,* Auge um Auge, S. 146.

[6] Vgl. *Daun,* Auge um Auge, S. 146.

[7] Vgl. *Burch*, S. 17ff; *Cowan*, S. 10ff; *Hulnick,* IJIC (22) 2009, S. 569ff; *Posner,* S. 67ff; *Rascoff,* S. Cal. L. Rev. (83) 2010, S. 575ff; *Treverton,* Reorganizing, S. 85ff. Zum Teil wird die Freistellung der DII von verfassungsrechtlichen Vorgaben gefordert.

lückenhaften Normierung des Geheimdienstrechts zu einer Reihe von Missbrauchsskandalen, welche durch die Überwachung der eigenen Bevölkerung ausgelöst wurden. Nach diesen Erfahrungen wird die geheimdienstliche Aufgabenwahrnehmung im Inland bis heute als Bedrohung der Bürgerrechte empfunden.[8] Die Skepsis der Bevölkerung gegenüber der Inlandsaufklärung verhinderte deren offizielle Einstufung als klassische Geheimdienstaufgabe. Im Gegensatz dazu wurde die Inlandsaufklärung in Deutschland mit dem Erlass des BVerfSchG im Jahr 1950 frühzeitig einer gesetzlichen Normierung zugeführt. Hierdurch konnten kompetenzwidrige Übergriffe stärker eingedämmt werden, sodass speziell gegenüber der Inlandsaufklärung kein vergleichbares Misstrauen entstand.

Ein dritter Grund beruht auf der unterschiedlichen Wahrnehmung terroristischer Bedrohungen. Während in Deutschland aufgrund linksterroristischer Strukturen die Inlandsaufklärung relativ früh eine wesentliche Aufgabe des Geheimdienstsektors bildete, wurden terroristische Bedrohungen in den USA lange Zeit nicht als Problem der inneren Sicherheit wahrgenommen. Nach dem amerikanischen Verständnis gingen Bedrohungen der nationalen Sicherheit lange Zeit vom Ausland aus, weshalb der Terrorismus ursprünglich nur als auslandspezifische Gefahr wahrgenommen wurde.[9] Die Schaffung einer eigenständigen, mit Sonderbefugnissen ausgestatteten Behörde schien dementsprechend nur in Bezug auf die Auslandsaufklärung erforderlich. Spätestens mit den Anschlägen von 2001 wurden jedoch die Gefahren extremistischer Strukturen im Inland deutlich. Im Vergleich dazu wurde in Deutschland die Notwendigkeit einer inlandsbezogenen Aufklärung sehr viel früher erkannt und vor allem durch Anschläge linksextremistischer Gruppierungen in den 1970er Jahren bestätigt.

C. Strukturelle Herausforderungen

Beide Geheimdienstsektoren sehen sich ähnlichen strukturellen Herausforderungen gegenüber. Sowohl das deutsche als auch das amerikanische Geheimdienstwesen sind im besonderen Maße zerklüftet. Dies erschwert die Zusammenarbeit der einzelnen Sicherheitsbehörden und die Verknüpfung der im Rahmen der geheimdienstlichen Informationserhebung gewonnenen Erkenntnisse. Während in Deutschland diese Zersplitterung überwiegend auf föderale Grundstrukturen zurückzuführen ist, spielt dieser Aspekt im amerikanischen Geheimdienstrecht keine Rolle. Dort beruht die Vielfalt des Geheimdienstsektors eher auf bürokratischen und systembedingten Prozessen. Diese unterschiedlichen Ursachen werden nachfolgend einander gegenübergestellt.

---

[8] Vgl. *Martin,* SAIS Review (24) 2004, S. 7.

[9] Vgl. *Zöller,* Terrorismusstrafrecht, S. 200.

Das deutsche Sicherheitswesen unterliegt einem föderalen Ordnungssystem. Diese Struktur setzt sich im Geheimdienstsektor fort und führt dort zu einer Zuständigkeitsaufteilung zwischen den verschiedenen Diensten auf Bundes- und Landesebene. Das amerikanische Rechtssystem ist ebenfalls föderalistisch organisiert. Allerdings beschränkt sich die offizielle amerikanische *Intelligence Community* auf Bundesbehörden, sodass das föderale Organisationsprinzip für die Gestaltung des amerikanischen Geheimdienstsektors nur eine untergeordnete Rolle spielt.[10] Die Zahl der mit Geheimdienstaufgaben betrauten Behörden hat im amerikanischen System eher schrittweise zugenommen. Angesichts der in den 1970er Jahren geschaffenen Kontrollmechanismen wurde der offizielle Geheimdienstsektor im Lauf der Zeit zunehmend um inoffizielle Akteure ergänzt, sodass eine erhebliche Zahl der amerikanischen Behörden über eigenständige Geheimdienstzweige verfügt.[11] Durch die Angliederung geheimdienstlicher Strukturen an schwächer kontrollierte Behörden sollte die Handlungsfähigkeit der Regierung in bestimmten Krisensituationen bewahrt werden.[12] Viele dieser Stellen wurden daher zunächst nur vorübergehend als Reaktion auf bestimmte Bedrohungslagen oder zur Bekämpfung bestimmter Gruppierungen eingeführt. Da sich die errichteten Behördenapparate allerdings nach Entfallen der für sie konstituierenden Gefahrenlage oftmals vehement gegen ihre Auflösung wehrten, blieben einige dieser Einrichtungen bestehen.[13] Wie erfolgreich sich amerikanische Einrichtungen gegen ihre Abschaffung zur Wehr setzen, verdeutlicht die fortwährende Existenz des *Counter Terrorism Center* (CTC).[14] Das CTC sollte im Jahr 2004 durch das *National Counter Terrorism Center* (NCTC) abgelöst werden. Es hat seine Existenzberechtigung jedoch bis heute verteidigt. Dadurch kam es zu einer Verdoppelung der für die Koordinierung der Sicherheitsbehörden zuständigen Stellen.[15] Damit werden bestimmte Überwachungsbereiche stärker als in Deutschland zeitgleich von mehreren Diensten abgedeckt.

D. Zusammenarbeit mit anderen Sicherheitsbehörden

Darüber hinaus scheint die Zusammenarbeit der verschiedenen Sicherheitsbehörden einem abweichenden Grundmodell zu folgen. In diesem Zusammenhang wird vereinzelt davon ausgegangen, dass sich das amerikanische Geheimdienst-

---

[10] Geheimdienste in Form der deutschen Landesverfassungsschutzämter sind damit grundsätzlich nicht vorgesehen.

[11] Vertiefend zu dieser Inkongruenz *Jäger/Daun,* in: Borchert, S. 60f. Zudem wurden den Polizeibehörden zum Teil ebenfalls *intelligence*-Befugnisse übertragen.

[12] So *Jäger/Daun,* in: Borchert, S. 61.

[13] So *Jäger/Daun,* in: Borchert, S. 60f.

[14] Vgl. etwa *Jäger/Daun,* in: Borchert, S. 63.

[15] Vgl. hierzu *Jäger/Daun,* in: Borchert, S. 71.

wesen durch ein stärkeres Konkurrenzdenken auszeichnet als das deutsche.[16] Danach folgt das amerikanische System einem kompetitiven Modell, während dem deutschen Recht ein Mischmodell aus kompetitiven und konsensorientierten Elementen zugrunde liegen soll.[17] Begründet wird diese Auffassung mit der im amerikanischen Geheimdienstwesen tief verwurzelten Identifikation mit der eigenen Behördenkultur, welche letztlich zu einem starken Konkurrenzverhältnis und damit zu einer Abschottung von anderen Behörden führe.[18] Bei einer Berücksichtigung der in der Vergangenheit bekannt gewordenen Überwachungsmaßnahmen wird jedoch deutlich, dass das deutsche Modell ebenfalls von einem massiven Konkurrenz- und Wettbewerbsverhältnis geprägt wird. Dies trat unter anderem durch den Untersuchungsausschuss zur Zwickauer Neonazi-Zelle zutage, der feststellte, dass erhebliche Mängel im Informationsaustausch eine Aufdeckung der Mordfälle verhinderten. Ausgehend von diesen Defiziten sind die Regierungen und Parlamente in beiden Rechtsordnungen bestrebt, die informationelle Zusammenarbeit der verschiedenen Behörden zu verbessern. Diese Bemühungen spiegeln sich jeweils im Aufbau neuer Koordinierungsgremien und der Schaffung neuer gesetzlicher Vorgaben wider, die einen intensiven Informationsaustausch gewährleisten sollen. Im deutschen Kontext wird dies beispielhaft an der ATD und dem GTAZ, im amerikanischen Kontext am Aufbau der *Information Sharing Environment* oder der JTTFs deutlich. Diese staatlichen Vorgaben werden jedoch weder von den deutschen noch von den amerikanischen Diensten im intendierten Maß angenommen.

E. Gestaltung des Geheimdienstrechts

Weitere Unterschiede ergeben sich in Bezug auf die Ausgestaltung des Geheimdienstrechts. Diese können in großen Teilen ebenfalls auf die verschiedenartige Rechts- und Sicherheitsarchitektur zurückgeführt werden. In Deutschland wird die Regelungsdichte der geheimdienstlichen Ermächtigungsgrundlagen durch das Trennungsgebot, die Unterscheidung von Kompetenzen zur Prävention und zur Repression und die Vorgaben des Gesetzesvorbehalts reguliert. In den USA werden die Strukturen demgegenüber durch die organisatorische Vormachtstellung des FBI und die Anforderungen des vierten Verfassungszusatzes bestimmt.

Diese unterschiedlichen Bedingungen führen dazu, dass in Deutschland das Recht der Geheimdienste mit den Nachrichtendienstgesetzen und dem G10 eine weitgehend einheitliche Kodifikation erfahren hat, während in den USA die Befug-

---

[16] Vgl. *Jäger/Daun,* in: Borchert, S. 61, 69.

[17] Vgl. *Jäger/Daun,* in: Borchert, S. 66; ebenso *Ziercke,* in: Bundesamt für Verfassungsschutz, S. 41, demzufolge Verfassungsschutz und Polizei „nicht in Konkurrenz zueinander" stehen.

[18] Insgesamt vertiefend *Best,* CRS 2011, summary, sowie S. 1.

nisse und Kompetenzen der einzelnen Geheimdienste weniger präzise reguliert sind.[19] Das amerikanische Geheimdienstrecht ist vielmehr durch eine große Anzahl von Einzelgesetzen geprägt.[20] Die Vorgaben des *National Security Act* bilden zwar ein einheitliches Regelwerk, sind jedoch zu vage formuliert, um eine konkrete Abgrenzung der einzelnen Ermittlungsbefugnisse zu erlauben.[21] Ein dem deutschen BVerfSchG vergleichbarer, allgemeiner Gesetzesteil besteht nicht, sodass die zahlreichen Definitionen in den einzelnen *Titles* des U.S.C. variieren können.

Ausgehend von den Erkenntnissen der Landesberichte werden die Auswirkungen der vorgenannten Besonderheiten nachfolgend vergleichend gegenübergestellt.

1. Kompetenzverteilung in nationalen Sicherheitsfragen

Einen ersten Erklärungsansatz liefern die abweichende Sicherheitsarchitektur und die damit einhergehende Kompetenzverteilung im Geheimdienstrecht. Im deutschen Rechtssystem ist die Aufteilung zwischen repressiven und präventiven Verfahrenszwecken von zentraler Bedeutung. Während das Straf- und Strafverfahrensrecht in die Kompetenz des Bundes fällt, sind präventive Aufgaben der Regelungskompetenz der Länder zuzuordnen.[22] Die Errichtung des präventiv tätig werdenden Bundesnachrichtendienstes war dementsprechend nur aufgrund ausdrücklicher Kompetenztitel im Grundgesetz möglich. Diese Zuständigkeitsaufteilung erklärt zudem, warum die Einbeziehung der OK in den Beobachtungsauftrag der Landesverfassungsbehörden nicht ausschließlich auf repressive Zwecke gestützt werden konnte, sondern eines gewissen Begründungsaufwandes bedurfte.[23]

In den USA ist die abweichende Gestaltung des Geheimdienstrechts wiederum durch den verfassungsrechtlichen Zuständigkeitsvorbehalt des Präsidenten in nationalen Sicherheitsfragen bedingt. Aufgrund dieser Vorbehaltsrechte hat der Kongress die Regulierung des Sicherheits- und Geheimdienstsektors weitgehend dem Präsidenten überlassen[24] und das amerikanische Recht wird daher maßgeblich durch dessen Anordnungen oder durch Richtlinien des Justizministeriums bestimmt.[25] Eine Aufteilung in präventive und repressive Verfahrenszwecke muss insofern nicht beachtet werden.

---

19 So *Scheppele,* Fordham L. Rev. (75) 2006, S. 617.

20 Lediglich für das KSA fehlt bislang eine gesetzliche Grundlage.

21 Vgl. *Hörauf,* S. 339.

22 Vgl. *Roggan,* in: Roggan/Kutscha, S. 217.

23 Zur Diskussion vgl. *Roggan,* in: Roggan/Kutscha, S. 416f.

24 Dem Präsidenten kommt insofern die Stellung als Oberbefehlshaber über die Streitkräfte zu, vgl. *Grunwald,* S. 31, 33, 68f.

25 Vgl. *Grunwald,* S. 40.

2. Auswirkungen von Gesetzesvorbehalt und Verfassungsgarantien

Ein zweiter Faktor ist der unterschiedliche Einfluss der nationalen Verfassungsgarantien. In Deutschland ist die hohe Regelungsdichte neben der Zuständigkeitsaufteilung zwischen Bund und Ländern den allgemeinen Vorgaben des Gesetzesvorbehalts geschuldet. Danach können wesentliche Grundrechtseingriffe nur bei Vorliegen einer hinreichend bestimmten und verhältnismäßigen Ermächtigungsgrundlage gerechtfertigt werden.[26] Dies macht im oftmals eingriffsintensiven Geheimdienstsektor regelmäßig eine klare Definition der Zuständigkeit erforderlich. Eine solche wird vor allem durch das BVerfSchG erreicht, das als zentrale Grundverweisungsnorm zu einer gewissen Vereinheitlichung beiträgt.

In den USA existiert demgegenüber kein dem deutschen Konzept vergleichbarer strenger Gesetzesvorbehalt.[27] Ein Regulierungsbedarf wird dort lediglich bei einer Beeinträchtigung von Verfassungsgarantien angenommen, sodass der Kongress nur vereinzelte Bereiche einer ausdrücklichen gesetzlichen Normierung zugeführt hat.[28] Eine solche verfassungsrechtlich notwendige Sonderregelung bildet etwa der FISA, der für Zwecke der auslandsbezogenen Inlandsaufklärung Ausnahmen von den strikten Vorgaben des vierten Verfassungszusatzes vorsieht. Der Anwendungsbereich dieses Gesetzes ist allerdings auf die Beobachtung von ausländischen und internationalen Bedrohungen beschränkt. Eine ausdrückliche Sonderermächtigung für die geheimdienstliche Überwachung rein inländischer extremistischer Bedrohungen und damit ein Äquivalent zu den deutschen Verfassungsschutzgesetzen fehlt.[29] Dementsprechend setzt sich das angesprochene institutionelle Vakuum im Bereich der Inlandsaufklärung auf Gesetzesebene fort. Aufgrund der gerichtlich festgestellten Bindung der *domestic intelligence investigations* an den vierten Verfassungszusatz wird diese Lücke im amerikanischen Recht trotz unterschiedlicher Zwecksetzung durch die Heranziehung strafrechtlicher Standards gelöst.[30] Dieser letztlich durch den vierten Verfassungszusatz bedingte Unterschied zum deutschen Modell wird am Beispiel der geheimdienstlichen Telekommunikationsüberwachung besonders deutlich. Diese unterliegt bei einem Auslandsbezug den Regeln des FISA, für rein inlandsbezogene Konstellationen ist ein Rückgriff auf die Ermächtigungen des *Title III* erforderlich. Im Vergleich dazu wurde für den deutschen Geheimdienstsektor mit dem G10 ein einheitlicher Standard geschaffen. Zwar wird dem BND als Auslandsnachrichtendienst mit der strategischen Überwachung ebenfalls ein Mehr an Befugnissen zugestanden. Die nachrichtendienst-

---

[26] BVerfG NJW 1979, S. 359f.

[27] Vertiefend zum Gesetzesvorbehalt und Rechtsstaatsverständnis im amerikanischen Recht *Lepsius,* S. 207ff; vgl. zudem *Grunwald,* S. 30.

[28] So *Ross,* in: Dubber, S. 138.

[29] Vgl. *Grunwald,* S. 76; *Rascoff,* S. Cal. L. Rev. (83) 2010, S. 575ff.

[30] Vgl. *Rascoff,* S. Cal. L. Rev. (83) 2010, S. 598, 604, 648.

lichen Befugnisse unterscheiden sich aber auch im Bereich der Individualüberwachung von den Möglichkeiten der Strafverfolgungsbehörden nach § 100a StPO.

3. Aktuelle Tendenzen

In beiden Rechtsordnungen werden die Regelungen des Geheimdienstrechts aktuellen Entwicklungen angepasst. In Deutschland wird dieser Trend an Schlagworten wie der Vernachrichtendienstlichung der Polizei deutlich, wonach die gesetzliche Annäherung beziehungsweise Ausweitung vor allem durch den Ausbau polizeilicher Befugnisse erfolgt. Einer umgekehrten Annäherung, das heißt der Verpolizeilichung der Nachrichtendienste, steht vor allem das Trennungsgebot entgegen.

In den USA zeichnen sich ebenfalls erhebliche Veränderungsprozesse ab. Da die polizeiliche Arbeit dort jedoch den strikten Vorgaben des vierten Verfassungszusatzes unterliegt, gehen die wesentlichen Impulse vom Geheimdienstsektor aus. So wurden etwa die Überwachungsmöglichkeiten nach dem FISA auf strafrechtliche Zwecke ausgedehnt.

III. Stellung der Geheimdienste in der Sicherheitsarchitektur

Die gegenwärtige Stellung der Geheimdienste in der nationalen Sicherheitsarchitektur ist in beiden Rechtsordnungen durch die Annäherung an andere Sicherheitsbehörden geprägt. Die unterschiedlichen Entwicklungsstufen werden in den nächsten Abschnitten unter einem vergleichenden Blickwinkel nachvollzogen.

A. Entwicklung nach 1945

Die im Ausgangspunkt vorgesehene Verortung der Geheimdienste in die Sicherheitsarchitektur unterscheidet sich in beiden Rechtsordnungen erheblich. Der Aufbau des deutschen Nachrichtendienstwesens nach dem Zweiten Weltkrieg wurde maßgeblich durch das Trennungsgebot und den Sicherheitsföderalismus geprägt. Diese Vorgaben bedingen die bis heute geltende Dreiteilung zwischen Geheimdiensten, Polizei und Strafverfolgungsbehörden. In den USA wurde demgegenüber durch den *National Security Act* von 1947 ein gemischtes Modell begründet. Dieses trennte zwischen den Bereichen der Inlands- und Auslandsaufklärung, während im Inland polizeiliche und geheimdienstliche Aufgaben einheitlich durch das FBI wahrgenommen wurden. Ausgehend von der ursprünglichen Verortung sind in der nachfolgenden Entwicklung zum Teil gegenläufige Tendenzen festzustellen. Die

Verschmelzung beider Bereiche in einer einzigen Behörde führte zu erheblichen innenpolitischen Schwierigkeiten. Nach Bekanntwerden zahlreicher Missbrauchsfälle wurde in den USA mit dem *primary purpose*-Test und der *wall* eine Beschränkung des Informationsaustauschs durchgesetzt. Dies wurde durch die kompetitive Ausrichtung des amerikanischen Geheimdienstsektors begünstigt, der sich in der Folgezeit nach dem *need to know*-Prinzip zunehmend von anderen Behörden abschottete.

Während diese Isolierung in den USA zunächst weiter gefestigt wurde, war die Entwicklung in Deutschland durch eine stete Annäherung gekennzeichnet. Ausgehend von den linksextremistischen Bestrebungen in den 1970er Jahren über die Zunahme der Organisierten Kriminalität in den 1980er Jahren bis hin zu den Bedrohungen des Terrorismus wurden die deutschen Nachrichtendienste Schritt für Schritt in ein ganzheitliches Sicherheitskonzept eingebunden. Die Angleichung der unterschiedlichen Sicherheitsbereiche erfolgte dabei sowohl von polizeilicher als auch von nachrichtendienstlicher Seite. Beispiele dieser Entwicklung sind unter anderem der Ausbau polizeilicher Vorfeldbefugnisse und heimlicher Ermittlungsmethoden, die Erweiterung des geheimdienstlichen Beobachtungsauftrags auf strafrechtlich relevante Bereiche sowie die Einräumung einer Befugnis zur Übermittlung an die Polizei und Staatsanwaltschaften.

B. Entwicklung nach 2001

Nach den Anschlägen von 2001 wird die Entwicklung in beiden Rechtsordnungen durch sehr ähnliche Tendenzen bestimmt. Im deutschen Sicherheitswesen wurden die bereits existierenden Annäherungstendenzen durch neue Kooperationsformen und gemeinsame Datensätze verstärkt. Im amerikanischen Recht kam es ebenfalls zu einer Annäherung der verschiedenen Sektoren. Da die Anschläge die Einbindung der Geheimdienste schlagartig in das politische Bewusstsein rückten, erfolgte dieser Wandel jedoch sehr viel schneller und radikaler als im deutschen Kontext. Als Konsequenz aus den aufgezeigten Sicherheitsdefiziten wurde etwa das *need to know*- durch das *need to share*-Prinzip abgelöst und die bisherigen Informationsgrenzen wurden durch eine Abschaffung des *primary purpose*-Tests und die Öffnung des FISA aufgehoben.[31] Die bis dato maßgebliche Unterscheidung zwischen inlands- und auslandsbezogenen Maßnahmen wurde hierdurch weitgehend bedeutungslos, was letztlich zu einer vollständigen Integration geheimdienstlicher Ermittlungen in das amerikanische Sicherheitswesen führte. Dieser komplette Wandel wurde auf die amerikanische Idee eines *war on terror* und damit auf eine Art Notstandsgesetzgebung gestützt.[32] Aufgrund der in nationalen Sicherheits-

---

[31] Vgl. zum Wandel zum *need to share Jones,* B.U. Pub. Int. L.J. (19) 2008, S. 152.

[32] Beispiele sind der USA PATRIOT Act von 2001 oder der MCA 2006.

fragen bestehenden präsidialen Befugnisse konnten vereinzelte Kategorien damit sehr einfach, fundamental und schnell geändert werden.[33] Während in Deutschland das Trennungsgebot und der grundrechtliche Zweckbindungsgrundsatz zumindest offiziell unangetastet bleiben sollten, wurde das amerikanische Geheimdienstwesen einem grundlegenden Wandel unterzogen.

C. Resümee zur aktuellen Rechtslage

Zwischen dem deutschen und amerikanischen Sicherheits- und Geheimdienstwesen bestehen sowohl in rechtlicher als auch in tatsächlicher Hinsicht weiterhin erhebliche Unterschiede. Gemeinsam ist beiden Rechtsordnungen jedoch, dass im Zuge verschiedener Reformen bislang traditionelle Grundstrukturen aufgegeben wurden. Die aktuelle Position der Geheimdienste ist dementsprechend sowohl im deutschen als auch im amerikanischen Recht maßgeblich durch die Reformen der vergangenen Jahre bestimmt. Aufgrund der national bedingt unterschiedlichen Gestaltungsvorgaben kommen die Entwicklungsimpulse aus jeweils verschiedenen Richtungen. Während im amerikanischen Kontext eine Verschmelzung der unterschiedlichen Sicherheitsbereiche durch eine Ausweitung der auslandsspezifischen Sonderbefugnisse und damit vonseiten der Geheimdienste erfolgt, findet diese Annäherung in Deutschland aufgrund des Trennungsgebots vor allem vonseiten des Polizei- und Strafverfolgungssektors statt.

Diese Entwicklung zielt zudem sowohl im deutschen als auch im amerikanischen Recht auf eine Annäherung der verschiedenen Sicherheitsbehörden. Im deutschen Modell werden zwar weiterhin die Kompetenzaufteilung des Sicherheitsföderalismus sowie die Vorgaben des Trennungsgebots betont, perspektivisch rücken die Nachrichtendienste jedoch mit den übrigen Sicherheitsbehörden immer näher zusammen. Durch eine Erweiterung des Beobachtungsauftrags, die Einräumung von Übermittlungsbefugnissen und die Einrichtung gemeinsamer Informationszentren beziehungsweise Datenbanken werden schließlich die informationelle Gewaltenteilung und das Trennungsgebot zunehmend infrage gestellt.

In den USA vollzog sich diese Entwicklung anders als in Deutschland nicht schrittweise, sondern in Form eines abrupten Systemwandels. Obwohl die Aufklärung rein inländischer Sachverhalte offiziell weiterhin dem vierten Verfassungszusatz unterliegt, wurde die Trennlinie zwischen der inlands- und auslandsbezogenen Aufklärung durch die Neufassung des FISA nach 2001 weitgehend ausradiert. Die Verschmelzung der verschiedenen Sicherheitsstrukturen erreicht im amerikanischen Recht damit eine größere Dimension als im deutschen Kontext.

---

[33] Die bisherige Zweckbegrenzung im FISA konnte z.B. durch eine sprachliche Anpassung und deren weitgehende richterliche Bestätigung umfassend abgeschafft werden.

IV. Auswirkungen der Sicherheitsarchitektur

In den Landesberichten wurden auch die Auswirkungen der Sicherheitsarchitektur auf die Besonderheiten geheimdienstlicher Ermittlungen untersucht. Dieser Einfluss ist in beiden Rechtsordnungen erheblich. In Deutschland sind insofern die Vorgaben des Trennungsgebots und des Sicherheitsföderalismus von Bedeutung. In den USA spielen wiederum die Anforderungen des vierten Verfassungszusatzes eine zentrale Rolle. Der nachfolgende Vergleich verdeutlicht diese Auswirkungen in Bezug auf die geheimdienstliche Informationserhebung, die Zusammenarbeit mit dem Strafverfolgungssektor und die Nutzung nachrichtendienstlicher Erkenntnisse im Strafverfahren.

A. Erhebung von Geheimdienstinformationen im Vergleich

Die vergleichende Gegenüberstellung der geheimdienstlichen Informationserhebung orientiert sich an der Gliederung der Landesberichte. Es werden daher die im Geheimdienstsektor zentralen Aufgabenfelder, Ermittlungsschwellen, Befugnisse und Kontrollmechanismen einander gegenübergestellt.

1. Vergleich der Aufgaben

In beiden Rechtsordnungen ist die Verteilung der konkreten Aufgabenfelder zu einem erheblichen Teil auf die jeweils vorzufindende Sicherheits- und Rechtsarchitektur zurückführbar. Zwar erfolgt gleichermaßen eine Differenzierung zwischen der Erhebung von Beweismaterial und Geheimdienstinformationen, die Ursachen hierfür sind jedoch entsprechend der abweichenden Sicherheitsarchitektur unterschiedlich. Im deutschen Recht sind das Trennungsgebot und die kompetenzrechtliche Unterscheidung zwischen präventiven und repressiven Aufgaben ausschlaggebend. Demgegenüber basieren die Aufgaben des amerikanischen Geheimdienstsektors vor allem auf den Vorgaben des ersten und vierten Verfassungszusatzes, ohne dass eine dem deutschen Recht vergleichbare Aufteilung existiert.

Entsprechend diesen unterschiedlichen Strukturvorgaben werden Abweichungen hinsichtlich der einzelnen Aufgabenfelder deutlich. In Deutschland fokussiert sich die Arbeit der Dienste infolge des Trennungsgebots primär auf die Sammlung und Auswertung von Informationen und damit auf einen eher passiven Beobachtungsauftrags.[34] Sie dürfen aktiv weder polizeiliche Gefahrenabwehr- noch strafrechtliche Verfolgungsmaßnahmen vorantreiben. Der konkrete nachrichtendienstliche Aufgabenbereich orientiert sich zudem an der kompetenzrechtlichen Aufteilung in

[34] Vgl. *Forkert-Hosser,* S. 69.

präventive und repressive Tätigkeitsfelder. Da die deutschen Nachrichtendienste dem präventiven Staatsschutz zugeordnet werden, sind ihnen strafverfolgende Maßnahmen grundsätzlich untersagt. In Deutschland existieren damit für polizeiliche, strafrechtliche und geheimdienstliche Aufgaben jeweils eigenständige Behörden, Aufgaben und Ermächtigungsgrundlagen.

In den USA sind die Dienste ebenfalls mit der Sammlung und Auswertung sicherheitsrelevanter Erkenntnisse betraut. Da im amerikanischen Recht allerdings keine dem Trennungsgebot vergleichbare Beschränkung existiert, kann ihnen zusätzlich die Ergreifung aktiver Gegenmaßnahmen gestattet werden. Eine Trennung geheimdienstlicher und polizeilicher Maßnahmen findet sich lediglich in Bezug auf die CIA, der Zwangs- und Polizeimaßnahmen sowie Überwachungsmaßnahmen im Inland verboten sind.[35] Dieses Verbot gilt jedoch ausschließlich für die CIA und findet auf die übrigen Geheimdienste keine Anwendung. Die geringe Reichweite des Vorbehalts wird unter anderem daran deutlich, dass das Verbot vor allem auf Drängen des FBI zum Erhalt seiner inlandsbezogenen Vormachtstellung zustande kam, während das FBI selbst über polizeiliche *und* geheimdienstliche Befugnisse verfügt. Der CIA-Vorbehalt besitzt damit anders als das deutsche Trennungsgebot keine verallgemeinerungsfähige Aussagekraft für das amerikanische Geheimdienstwesen und kann dementsprechend nicht auf den übrigen Geheimdienstsektor übertragen werden. Darüber hinaus ist die Vorgabe selbst für die CIA nur teilweise wirksam, da der Umfang der zulässigen inländischen Aktivitäten weder durch den Kongress noch durch die Gerichte eindeutig festgelegt wurde.[36] Lediglich das Verbot inländischer Tätigkeit wird in der E.O. 12333 von 2008 unter Punkt 2.4(a) dahingehend präzisiert, dass der Einsatz elektronischer Überwachungsmaßnahmen durch die CIA im Inland ausgeschlossen ist. Im Übrigen ist weitgehend unklar, welche Befugnisse die CIA gegen wen und wo einsetzen darf.[37] Von diesem Sonderfall abgesehen unterliegt das Aufgabenspektrum der amerikanischen Geheimdienste – mangels Trennungsgebot – einer vom deutschen Recht grundsätzlich abweichenden Einteilung.

Im amerikanischen Recht bestimmen sich die geheimdienstlichen Betätigungsmöglichkeiten eher an verfassungsrechtlichen Strukturvorgaben. Während geheimdienstliche Ermittlungen mit Auslandsbezug beispielsweise weitgehend von den Regelungen des vierten Verfassungszusatzes befreit sind, müssen rein inländische Aufklärungs- und Strafverfolgungsmaßnahmen grundsätzlich den Vorgaben der Verfassungsnorm genügen. Werden diese Anforderungen nicht eingehalten, sind

---

[35] Siehe 50 U.S.C. § 403-4A(d)(1).

[36] *Harris,* Yale L. & Pol'y Rev. (23) 2005, S. 533f; *Hörauf,* S. 291, *Ortiz,* in: Markle Foundation, S. 95. So stellt das Gericht in *Fitzgibbon v. CIA*, 911 F.2d 755, 764 (D.C. Cir. 1990) fest, "that the Agency must, at times, pursue domestically its foreign intelligence mandate".

[37] So etwa *Harris,* Yale L. & Pol'y Rev. (23) 2005, S. 533.

die Erkenntnisse gegebenenfalls als *intelligence,* nicht jedoch als *evidence* verwertbar. Damit wird im amerikanischen Recht zum Teil ebenfalls zwischen der Erhebung von Beweismaterial und Geheimdienstinformationen unterschieden. Die zur Anwendung kommenden Erhebungsstandards orientieren sich jedoch anders als in Deutschland nicht an den Kompetenzgrenzen unterschiedlicher Behörden, sondern an taktischen Erwägungen innerhalb einer Behörde. Eine Ermittlungsbehörde wie das FBI entscheidet danach selbst, ob sie im Rahmen des *law enforcement*- oder des *intelligence*-Auftrags durch die Einhaltung der Ermittlungsstandards potentiell verwertbares Beweismaterial erhebt oder nicht.[38] Die im deutschen und amerikanischen Geheimdienstwesen unterschiedlichen Aufgabenspektren sind damit zu einem erheblichen Teil auf die jeweils vorzufindende Sicherheits- und Rechtsarchitektur zurückführbar.

2. Vergleich der Befugnisse und Durchsetzungsmöglichkeiten

Daneben wurden die geheimdienstlichen Ermittlungsmethoden und Durchsetzungsmöglichkeiten untersucht. In beiden Rechtsordnungen stehen den Geheimdiensten vergleichbare Ermittlungsbefugnisse zur Verfügung, welche sich in gleicher Weise durch eine gewisse Entwicklungsoffenheit auszeichnen. Zudem wurden diese Befugnisse in beiden Ländern nicht nur ausgebaut, sondern auch anderen Ermittlungsbehörden zugänglich gemacht. Aufgrund der Öffnung beider Geheimdienstsektoren sind viele geheimdienstliche Befugnisse nicht mehr ausschließlich den klassischen Produzenten von Geheimdienstinformationen vorbehalten. Unterschiede ergeben sich im Grad dieser Öffnung sowie den Durchsetzungsmöglichkeiten, die den nationalen Geheimdiensten zur Verfügung stehen. Diese Gemeinsamkeiten und Unterschiede werden nachfolgend unter Rückgriff auf die Erkenntnisse der Landesberichte nachvollzogen.

a) Allgemeine Annäherungstendenzen

Der in den Landesberichten zunächst vorgenommene landesinterne Vergleich zwischen dem Geheimdienstsektor und dem nationalen Polizei- und Strafverfolgungssektor verdeutlicht Eigenheiten wie Berührungspunkte. Demnach sind sowohl in den USA als auch in Deutschland viele geheimdienstliche Befugnisse nicht (mehr) exklusiv zur Erhebung von Geheimdienstinformationen ausübbar. Ausgehend vom deutschen Sicherheitsföderalismus müssen die deutschen Sicherheitsbehörden jedoch selbst bei parallelen Ermittlungsbefugnissen auf eigenständige, von den Nachrichtendienstgesetzen getrennte Ermächtigungsgrundlagen zurückgreifen. Diese strikte Unterscheidung besteht im amerikanischen Recht nicht. Dort kann

---

[38] Zur Differenzierung zwischen *law enforcement* und *intelligence* vgl. *Fredman,* Yale L. & Pol'y Rev. (16) 1998, S. 337; *Treverton,* Intelligence, S. 1f.

sich das FBI etwa unter den Voraussetzungen des aktuellen *significant purpose*-Standards auch zu Strafverfolgungszwecken auf den FISA stützen.

b) Umfang geheimdienstlicher Befugnisse

Bei einer Gesamtbetrachtung der im deutschen und amerikanischen Geheimdienstsektor zur Verfügung stehenden Ermittlungsmethoden ergibt sich wiederum ein homogenes Bild: Die deutschen und amerikanischen Dienste besitzen weitgehend vergleichbare Ermittlungsbefugnisse. Diese können mit der Erhebung aus offen zugänglichen Quellen, der heimlichen Informationsbeschaffung, der Einschleusung von Informanten und Ermittlern und dem Einsatz technischer Überwachungsmethoden in jeweils vier Kategorien eingeteilt werden. Die Durchführung verdeckter Ermittlungen,[39] die akustische und optische Wohnraumüberwachung,[40] die Abfrage von Verkehrs-, Bestands-, und Kundendaten[41] sowie der Zugriff auf Inhaltsdaten von Telekommunikationsvorgängen[42] können von Geheimdiensten beider Rechtsordnungen wahrgenommen werden.

c) Entwicklungsoffenheit geheimdienstlicher Methoden

Beide Systeme zeichnen sich zudem durch eine Entwicklungsoffenheit des geheimdienstlichen Methodenspektrums aus. Sowohl in den USA als auch in Deutschland können flexibel neue Ermittlungsmaßnahmen eingeführt werden. In Deutschland ist diese Möglichkeit in § 8 II 2 BVerfSchG vorgesehen. Dieser erlaubt der Exekutive, in einer Dienstvorschrift neue Methoden und Instrumente heimlicher Informationsbeschaffung zu benennen.[43] Eingriffsintensive Methoden allerdings[44] müssen aufgrund des Gesetzesvorbehalts formal in den Nachrichtendienstgesetzen festgelegt werden. Die im amerikanischen Modell bestehenden Handlungsspielräume sind im Vergleich zum deutschen Ansatz weiter. Dort ist der Präsident in bestimmten Fällen zur Einräumung neuer geheimdienstlicher Überwachungsmethoden befugt. Auf diese präsidiale Befugnis wurden selbst eingriffsintensive Maßnahmen wie das *NSA-Surveillance Program* gestützt.[45]

---

[39] Nach den §§ 8 II, 9 I BVerfSchG bzw. den Mukasey Guidelines 2008.

[40] Nach den §§ 8 II, 9 II 1 und 2 BVerfSchG bzw. 50 U.S.C. § 1801(f) und (n).

[41] Vgl. die § 8a II Nr. 4, 5, § 9 IV BVerfSchG bzw. die 50 U.S.C. §§ 1841–1846, sowie §§ 1861–1863.

[42] Nach den §§ 1, 3 G10 bzw. 50 U.S.C. 1801–1812.

[43] Vgl. *Rose-Stahl,* S. 70.

[44] Vgl. *Hefendehl,* GA 2011, S. 212.

[45] Vgl. die Erklärung des *Attorney General Gonzales* vom 19.1.2006 mit dem Titel "Legal Authorities Supporting the Activities of the National Security Agency Described by the President" und die Erklärung des U.S. Department of Justice vom 27.1.2006 mit dem Titel

d) Durchsetzungsmöglichkeiten

Deutliche Unterschiede ergeben sich bezüglich der im Geheimdienstsektor bestehenden Durchsetzungsmöglichkeiten. Aufgrund der Vorgaben des Trennungsgebots verfügen die deutschen Nachrichtendienste, anders als ihre amerikanischen Pendants, nicht über polizeiliche Zwangsbefugnisse.[46] Sie dürfen lediglich Informationen sammeln.[47] Das Trennungsgebot findet im amerikanischen Geheimdienstrecht keine Entsprechung – die meisten amerikanischen Geheimdienste können auf typische polizeiliche Maßnahmen zurückgreifen und beispielsweise Personen und Räume zu geheimdienstlichen Zwecken durchsuchen.[48] Der CIA sind mit den sogenannten *covert actions* sogar die aktive politische Einflussnahme und die Durchführung paramilitärischer Operationen gestattet. Eine vergleichbare Befugnis für den BND ist vor dem historischen Hintergrund des deutschen Nachrichtendienstwesens undenkbar.

e) Ausbau bestehender Befugnisse

Abgesehen von den punktuellen Gemeinsamkeiten und Unterschieden ist in beiden Rechtsordnungen eine Tendenz zum Ausbau bestehender Ermittlungsbefugnisse feststellbar. In Deutschland hat der Gesetzgeber mit den Sicherheitspaketen von 2001 und 2002 sowie den Terrorismusbekämpfungs- und Ergänzungsgesetzen die Erhebungs- und Speicherungsbefugnisse der Sicherheitsbehörden stetig erweitert. Zuletzt wurden im Jahr 2011 beispielsweise die Auskunftsmöglichkeiten nach § 8a BVerfSchG ergänzt.[49] Noch umfassender waren die Reformen im amerikanischen Geheimdienstsektor. Dort wurden mit dem *USA PATRIOT Act* von 2001, dem *Homeland Security Act* von 2002, dem *Intelligence Reform and Terrorism Prevention Act* von 2004, dem *Protect America Act* von 2007 und dem *FISA Amendment Act* von 2008 neue Behörden, Kooperationsformen, Befugnisse und Austauschmöglichkeiten eingeführt.

Die kritische Resonanz fällt in beiden Rechtsordnungen sehr unterschiedlich aus. Die massiven Eingriffe in das amerikanische Geheimdienstwesen werden von den amerikanischen Gerichten kaum thematisiert. Lediglich der reformierte FISA wurde in der sogenannten *Mayfield*-Entscheidung von 2007 durch ein Gericht bean-

---

"The NSA Program to Detect and Prevent Terrorist Attacks: Myth v. Reality", zu finden unter http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf [Stand: 1.5.2012].

[46] Vgl. *Hörauf,* S. 19.

[47] Vgl. *Schafranek,* S. 81.

[48] Siehe 50 U.S.C. §§ 1821–1829; vgl. *Jäger/Daun,* in: Borchert, S. 62; ebenso *Grunwald,* S. 121, für das FBI. Einzige Ausnahme ist die CIA.

[49] Gleichzeitig wurde das Auskunftsrecht nach § 8a II Nr. 3 BVerfSchG bzgl. Postdienstleistungen gestrichen.

standet.[50] In Deutschland waren die verabschiedeten Sicherheitsgesetze demgegenüber Gegenstand zahlreicher und vor allem erfolgreicher Verfassungsbeschwerden. Beispiele sind unter anderem das Urteil des Sächsischen Verfassungsgerichtshof zum „Großen Lauschangriff" durch den Verfassungsschutz im Jahr 2005 oder das Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten im Jahr 2010.[51] Die ausufernde geheimdienstliche Informationsgewinnung wird zwar auch in den USA problematisiert, diese Auseinandersetzung findet hier allerdings fast ausschließlich in der akademischen Diskussion statt, während die Gerichte und die Rechtspraxis dem Ausbau der *information sharing environment* weiterhin positiv gegenüberstehen.

3. Vergleich der zeitlichen Rahmenbedingungen

Die Zuordnung der geheimdienstlichen Ermittlungsschwellen erfolgt in beiden Rechtsordnungen entlang der durch die Sicherheitsarchitektur vorgegebenen Strukturen. In beiden Ländern dürfen die Geheimdienste frühzeitig und grundsätzlich im Vorfeld strafbaren Handelns tätig werden. Der umfassende Beobachtungsauftrag wird mit dem Schutz überragend wichtiger Rechtsgüter sowie außen- und sicherheitspolitischen Belangen begründet. Die Einteilung der jeweils geltenden Ermittlungsschwellen orientiert sich an den Gestaltungsvorgaben des nationalen Rechts. In deutschem Kontext setzt sich die Dreiteilung zwischen polizeilichen, strafrechtlichen und geheimdienstlichen Maßnahmen auch hinsichtlich der Ermittlungsschwellen fort. Entsprechend den Regelungen des Gesetzesvorbehalts erfolgt, je nach Schwere der Erhebungsmaßnahme, eine Erhöhung der maßgeblichen Ermittlungsschwellen.

Diese Vorgaben finden in den USA keine Entsprechung. Dort orientieren sich die Ermittlungsschwellen primär an den richterlichen Präzisierungen des vierten Verfassungszusatzes, die bei Maßnahmen der FII abgesenkte Standards vorsehen. Die zeitlichen Rahmenbedingungen der deutschen und amerikanischen Geheimdienste werden damit ebenfalls durch die nationalen Gestaltungsvorgaben des Sicherheitswesens beeinflusst.

Dies gilt in gleicher Weise für das Ende geheimdienstlicher Ermittlungen. Dieses wird in beiden Rechtsordnungen sehr offen gehalten. Anders als im deutschen Kontext handelt es sich hierbei allerdings um kein signifikantes Merkmal der Geheimdienste, da in den USA die Geheimdienste und Strafverfolgungsbehörden gleichermaßen dem Grundsatz der Opportunität unterliegen.

Die Erkenntnisse zum Beginn und Ende geheimdienstlicher Ermittlungen werden in den nachfolgenden Abschnitten detailliert gegenübergestellt.

---

[50] Vgl. *Mayfield v. United States*, 504 F. Supp. 2d 1023, 1036ff (D. Or. 2007).

[51] Siehe SächsVerfGH NVwZ 2005, S. 1310, und BVerfG NJW 2010, S. 833.

a) Beginn geheimdienstlicher Ermittlungen im Vergleich

Der Beginn geheimdienstlicher Überwachungsmaßnahmen ist in beiden Rechtsordnungen tendenziell an sehr geringe Ermittlungsschwellen gebunden.

aa) Auswirkungen der Sicherheitsarchitektur

In deutschem Kontext setzt sich die Dreiteilung zwischen polizeilichen, strafrechtlichen und geheimdienstlichen Maßnahmen auch im Bereich der Ermittlungsschwellen fort. Im landesinternen Vergleich sind die geheimdienstlichen Ermittlungsschwellen rein theoretisch weiterhin von der polizeilichen Gefahrenschwelle und dem strafprozessualen Anfangsverdacht unterscheidbar. Innerhalb des Geheimdienstsektors gelten über die Grundverweisungsnorm des BVerfSchG wiederum sehr ähnliche Ermittlungsschwellen. Bei einfachen Erhebungsbefugnissen genügt insofern meist die Erforderlichkeit für die Aufgabenerfüllung, während bei heimlichen Beobachtungsmaßnahmen regelmäßig zumindest eine geringe Tatsachenbasis erforderlich ist. Lediglich die strategische Überwachung nach dem G10 erlaubt eine anlassunabhängige, sachbezogene Überwachung.

Im amerikanischen Recht orientieren sich die Ermittlungsschwellen ebenfalls an den bereits bekannten Strukturvorgaben. Stark vereinfacht kann zwischen drei Schwellen unterschieden werden. Diese betreffen erstens Maßnahmen außerhalb des vierten Verfassungszusatzes, zweitens Maßnahmen im Anwendungsbereich des vierten Verfassungszusatzes mit rein *inländischen* Bezug und drittens Maßnahmen im Anwendungsbereich des vierten Verfassungszusatzes mit *Auslands*bezug. Bei Ermittlungen der ersten Kategorie, das heißt abseits der Verfassungsgarantie, sind die amerikanischen Ermittlungsbehörden generell nicht an einen Verdachtsgrad oder die Darlegung bestimmter Anhaltspunkte gebunden.[52] Dies gilt selbst für die amerikanischen Strafverfolgungsbehörden, denen hierdurch der präventive Einsatz strafprozessualer Mittel unproblematisch gestattet ist.[53] Die im deutschen Recht charakteristische Vorfeldkompetenz der Geheimdienste stellt im amerikanischen Kontext folglich keine Besonderheit des Geheimdienstwesens dar. Die Differenzierung von geheimdienstlichen und strafrechtlichen Ermittlungen anhand der unterschiedlichen Verfahrenszwecke ist im amerikanischen Recht nicht vorgesehen. Gemeinsamkeiten zum deutschen Recht bestehen jedoch dahingehend, dass beide Rechtsordnungen einzelne geheimdienstliche Maßnahmen unabhängig von einer bestimmten Verdachtsbasis zulassen. In den USA ergibt sich die Reichweite dieser Fallgruppe im Umkehrschluss aus den vom vierten Verfassungszusatz erfassten Methoden. In Deutschland sind diese nur in gesetzlich normierten Ausnahmefällen

---

[52] Vgl. *Grunwald,* S. 253.

[53] Vgl. *Ross,* in: Dubber, S. 138.

wie der strategischen Überwachung oder bei fehlender Eingriffsintensität vorgesehen. Die Fallgruppe ist im amerikanischen Recht damit potentiell weiter gefasst als im deutschen Kontext.

Die für das amerikanische Geheimdienstrecht ebenfalls erwähnte zweite beziehungsweise dritte Ermittlungsschwelle greift, sobald der Anwendungsbereich des vierten Verfassungszusatzes eröffnet ist. In dieser Verfassungsgarantie wurde durch die höchstrichterliche Rechtsprechung ein zweispuriger Maßstab verankert, der zwischen rein inlandsbezogenen (DII und LEC) und auslandsbezogenen Ermittlungen (FII) unterscheidet. Bei rein inländischen Sachverhalten gelten für polizeiliche und geheimdienstliche Ermittlungen identische Rahmenbedingungen. Für das FBI verzichten die *Mukasey Guidelines* von 2008 dementsprechend ausdrücklich auf eine Differenzierung zwischen den einzelnen Bereichen. Sie stellen mit den *threat assessments,* den *preliminary investigations* und den *full investigations* einheitliche Standards für FBI-Operationen im Inland auf. Das FBI kann folglich sowohl geheimdienstliche als auch polizeiliche Ermittlungen aufgrund identischer Ermittlungsschwellen durchführen. Der für eine inlandsbezogene *search and seizure*-Maßnahme erforderliche Verdachtsgrad erscheint bei einer vergleichenden Betrachtung zunächst höher als derjenige der tatsächlichen Anhaltspunkte im deutschen Verfassungsschutzrecht. Allerdings werden beide Schwellen nicht als starre Grenzen verstanden, sondern meist einer Abwägung zugänglich gemacht. Durch diese Flexibilität erhalten beide Standards eine vergleichbare Weite, sodass die im Geheimdienstsektor geltenden Ermittlungsschwellen eine gewisse Ähnlichkeit aufweisen. Während im amerikanischen Recht allerdings für Maßnahmen der DII und der LEC einheitliche Standards zur Anwendung kommen, sind die Ermittlungsschwellen der deutschen Dienste im Vergleich zu anderen Sicherheitsbehörden zumindest theoretisch weiterhin abgesenkt und davon unterscheidbar.

Die dritte Schwelle des amerikanischen Geheimdienstrechts greift bei Maßnahmen mit Auslandsbezug. Diese unterliegen nur teilweise dem Anwendungsbereich des vierten Verfassungszusatzes, was eine Absenkung der Ermittlungsschwellen ermöglicht. Von dieser Option wurde im FISA vor allem in Bezug auf *Non-U.S. Persons* Gebrauch gemacht. Nicht dauerhaft zum Aufenthalt berechtigte Ausländer können selbst im Inland viel leichter Gegenstand einer geheimdienstlichen Überwachung werden als *U.S. Persons*. In Deutschland existieren mit der Inlands- und Auslandsaufklärung zwar ebenfalls unterschiedliche Zuständigkeiten und Maßstäbe, eine innerhalb einer Ermächtigungsgrundlage erfolgende Differenzierung zwischen Bürgern und Nichtbürgern ist im deutschen Recht dagegen nicht vorgesehen. Bei der Überwachung eines deutschen Staatsbürgers und eines Ausländers kommen grundsätzlich identische Ermittlungsstandards zur Anwendung.[54]

---

[54] Vgl. *T. Walter,* RIDP/IRPL 2009, S. 173.

bb) Bezugspunkte der Ermittlungsschwellen

Daneben unterscheiden sich die Bezugspunkte der jeweiligen Ermittlungsschwellen. Während im deutschen Geheimdienstrecht einheitlich ein weitgehend organisationsbezogener Ansatz verfolgt wird, differenziert das amerikanische Recht erneut zwischen den Strukturvorgaben des vierten Verfassungszusatzes. Dieser Unterschied erklärt sich erneut vor dem Hintergrund der unterschiedlichen Sicherheitsarchitektur. Da im amerikanischen Recht die Inlandsaufklärung tendenziell dem Polizei- und Strafverfolgungssektor zugeordnet wird, kommen für diesen Bereich konsequenterweise die aus dem Polizei- und Strafverfolgungssektor bekannten Voraussetzungen zur Anwendung. Aufklärungsmaßnahmen nach dem FISA haben wiederum einen anderen Bezugspunkt.

Im Einzelnen werden bei einer vergleichenden Gegenüberstellung die nachfolgenden, unterschiedlichen Bezugspunkte deutlich:

- Die Beobachtungen deutscher Nachrichtendienste sind nicht auf strafbare Vorgänge begrenzt, sondern richten sich auch auf organisationsbezogene und zweckgesetzte Verhaltensweisen. Eine Überwachung von Einzelpersonen ist im Rahmen der deutschen Inlandsaufklärung nicht als Regelfall vorgesehen, sondern nur unter den erhöhten Voraussetzungen des § 4 I 4 BVerfSchG möglich.
- In den USA liegt den rein inlandsbezogenen Überwachungsmaßnahmen der DII demgegenüber ein objektiver Tat- beziehungsweise Gefahrbezug zugrunde. Dieser Bezugspunkt deckt sich mit den für strafrechtliche Ermittlungen geltenden Anknüpfungspunkten amerikanischer und deutscher Strafverfolgungsbehörden. Eine Überwachung von Einzelpersonen ist im Bereich der DII nicht ungewöhnlich.
- Im Bereich der FII und damit vor allem bei Maßnahmen im Anwendungsbereich des FISA wird schließlich nicht primär auf eine bestimmte Verhaltensweise, sondern den Status als Agent einer ausländischen Macht abgestellt.[55] Für eine FISA-Maßnahme ist demensprechend ein Nexus nicht zwischen *Straftat* und überwachtem Ort, sondern zwischen *Zielobjekt* und überwachtem Ort erforderlich.[56] Im Gegensatz zum deutschen Nachrichtendienstrecht ist die Beobachtung bestimmter Personen im FISA von vorneherein angelegt. Dieser Unterschied wird etwa bei einem Vergleich der Telekommunikationsüberwachung nach dem FISA und dem G10 deutlich. Die Individualkontrolle nach §§ 1, 3 G10 fordert neben Gefahren für die freiheitliche demokratische Grundordnung zusätzlich den Verdacht auf eine Katalogtat beziehungsweise eine Mitgliedschaft in einer verfassungsfeindlichen Vereinigung. Demgegenüber knüpfen die FISA-Überwachungen primär an die Tauglichkeit des Beobachtungsobjekts als Agent einer ausländischen Macht an. Bei genauerer Betrachtung relativiert sich dieser Unter-

---

[55] Vgl. insgesamt *Baker,* Foreign Policy (97) Winter 1994–1995, S. 41.

[56] Vgl. *Kris/Wilson,* § 11:6, S. 407.

schied jedoch, da auch die FISA-Regeln die Agenteneigenschaft über Delikte des internationalen Terrorismus und des Waffenhandel und damit strafbares Verhalten definieren.[57] Die dort genannten Straftaten werden im Anwendungsbereich der §§ 1 und 3 G10 zum Teil ebenfalls anerkannt. Zudem lässt § 3 G10 die Mitgliedschaft in einer verfassungsfeindlichen Vereinigung in ähnlicher Weise genügen und knüpft damit die Überwachung nicht nur an das Verhalten, sondern zugleich an die Eigenschaft des Verdächtigen. Durch die Einbeziehung von Straftaten, wie beispielsweise die Einreise unter einer falschen Identität oder die Mitgliedschaft in einer ausländischen politischen Organisation, ist der Bezugspunkt des FISA aber weiterhin umfassender als derjenige des deutschen Geheimdienstrechts. Schließlich wird im deutschen Recht nicht zwischen inländischen und ausländischen extremistischen Organisationen differenziert. Die Bezugspunkte der für die deutschen und amerikanischen Dienste geltenden Ermittlungsschwellen weichen damit in zentralen Bereichen voneinander ab.

b) Ende geheimdienstlicher Ermittlungen im Vergleich

In beiden Rechtsordnungen wird den Geheimdiensten bei der Wahrnehmung ihres Beobachtungsauftrags ein umfassender Handlungsspielraum eingeräumt. Diese können selbst bei Bekanntwerden einer Straftat ihre Beobachtungen fortführen. Diese Ermittlungsgrenze stellt in der deutschen Sicherheitsarchitektur ein wesentliches Unterscheidungskriterium der Nachrichtendienste zu den Strafverfolgungsbehörden dar, da letztere im Gegensatz zu den Nachrichtendiensten an das Legalitätsprinzip gebunden sind. Lediglich bei schweren Delikten kann sich dieser Spielraum unter Umständen zu einer Übermittlungspflicht verengen. Die Außerkraftsetzung des Legalitätsprinzips im Geheimdienstwesen wird im deutschen Recht für gerechtfertigt gehalten, da das Trennungsgebot den gleichzeitigen Einsatz von Zwangsbefugnissen verhindert und die Dienste auf eine eher passive Informationserhebung zurückwirft.[58] Dieses Verständnis geht allerdings davon aus, dass die Geheimdienste nicht strafverfolgend tätig werden.[59]

In den USA werden die Geheimdienste in ihrem Beobachtungsauftrag zeitlich ebenfalls nicht eingeschränkt, sodass der Beendigungszeitpunkt geheimdienstlicher Ermittlungen in beiden Rechtsordnungen sehr ähnlich ausgestaltet ist. Anders als im deutschen Kontext handelt es sich hierbei allerdings um kein alleiniges Merkmal des Geheimdienstsektors, da dort die Geheimdienste und Strafverfolgungsbehörden gleichermaßen dem Grundsatz der Opportunität unterliegen.

---

[57] 50 U.S.C. § 1801.

[58] Vgl. *Forkert-Hosser,* S. 68.

[59] Vgl. *Roggan,* in: Roggan/Kutscha, S. 420f.

c) Allgemeine Tendenzen im Vergleich

In beiden Rechtssystemen wird eine allgemeine Tendenz zur Vorverlagerung beziehungsweise Aufweichung der traditionellen Ermittlungsschwellen deutlich. Beide Länder versuchen damit dem sicherheitspolitischen Bedürfnis nach einem funktionierenden Frühwarnsystem gerecht zu werden. Während der deutsche Gesetzgeber dieses Ziel durch die Einfügung neuer Ermittlungsschwellen verfolgt, setzen die USA auf eine Absenkung bisheriger Erhebungsstandards.[60] In beiden Rechtsordnungen stehen diese Entwicklungen im Widerspruch zu den klassischen Vorgaben der nationalen Sicherheitsarchitektur. In Deutschland werden in dieser Hinsicht die ehemals den Nachrichtendiensten vorbehaltenen Vorfeldbefugnisse durch Anpassungen des materiellen und des prozessualen Rechts zunehmend auch den Polizei- und Strafverfolgungsbehörden zugestanden. Diese Ergänzung der bestehenden Ermittlungsschwellen stellt nicht nur das Vorfeldmonopol der Nachrichtendienste infrage, sondern verwischt zugleich die traditionelle Trennlinie zwischen Prävention und Repression.[61]

In den USA sind trotz abweichender Rahmenbedingungen vergleichbare Aufweichungstendenzen erkennbar. Der Ausbau der Vorfeldstrafbarkeit wird dort etwa durch Straftatbestände des *material supports* massiv vorangetrieben. Daneben wurden durch die Abschaffung der *wall* die Besonderheiten der auslandsbezogenen Aufklärung auch auf andere Ermittlungstätigkeiten ausgeweitet, wodurch die ehemals nur im FISA enthaltenen Ermittlungsschwellen weitgehend ihren Sondercharakter verloren haben. Schließlich verwässern Änderungen wie das *lone wolf amendment* den normalerweise erforderlichen Organisationsbezug zugunsten personeller Elemente.

4. Vergleich materieller Erhebungsvoraussetzungen

Bei einer vergleichenden Gegenüberstellung der materiellen Erhebungsvoraussetzungen muss einerseits zwischen den Besonderheiten geheimdienstlicher Ermächtigungen innerhalb des jeweiligen Sicherheitswesens sowie anderseits zwischen dem deutschen und amerikanischen Geheimdienstsektor insgesamt unterschieden werden. Innerhalb beider Landesberichte sind Abstufungen zwischen geheimdienstlichen Erhebungsvoraussetzungen und Ermittlungsvoraussetzungen sonstiger Sicherheitsbehörden feststellbar. Im deutschen Kontext weichen die Anforderungen des Geheimdienstsektors einheitlich von den meist höheren Ermittlungsvoraussetzungen der Polizei- und Strafverfolgungsbehörden ab. In den USA beschränken sich die Unterschiede demgegenüber auf Geheimdienstmaßnahmen

---

[60] Vgl. hierzu *Hörauf,* S. 338f.

[61] So *P.-A Albrecht,* StV 2001, S. 417; *Grafe,* S. 9; *Wolff,* S. 34.

mit Auslandsbezug (FII), was vor allem am Beispiel des FISA deutlich wird. Im amerikanischen Recht kommen damit erneut die abweichenden Bedingungen rein inlandsbezogener (DII beziehungsweise LEC) und auslandsbezogener Maßnahmen (FII) zum Tragen. Die Anordnungsvoraussetzungen der FII nehmen hierbei eine Sonderstellung ein, während für rein inlandsbezogene Maßnahmen weitgehend identische Voraussetzungen gelten. Die Erhebungsvoraussetzungen des deutschen und amerikanischen Geheimdienstwesens folgen daher prinzipiell dem durch die Sicherheitsarchitektur vorgezeichneten Muster.

Abseits des internen Vergleichs zeigen sich bei einer Gegenüberstellung des deutschen und amerikanischen Geheimdienstrechts weitere Auffälligkeiten, die sowohl auf die unterschiedliche Gestaltung der Sicherheitsarchitektur als auch die Eigenarten des jeweiligen Rechtssystems zurückführbar sind. Im Bereich der allgemeinen Erhebungsvoraussetzungen enthalten beide Rechtsordnungen Vorschriften, welche die Informationserhebung an gewisse Verhältnismäßigkeitsvoraussetzungen koppeln. Davon abgesehen sind aufgrund unterschiedlicher Individualschutzkonzepte erhebliche Abweichungen erkennbar. Ausgehend von den Vorgaben des vierten Verfassungszusatzes erfolgt im amerikanischen Recht eine vom deutschen Ansatz abweichende Differenzierung zwischen den jeweiligen Beobachtungssubjekten und Ermittlungsmethoden. Ein Schutz von Individualrechten wird dort nicht für erforderlich gehalten, solange kein formelles Verfassungsrecht verletzt wird. Der deutsche Ansatz folgt demgegenüber einer Grundrechtsdogmatik, die sich unter anderem an der materiellen Intensität des Eingriffs orientiert. Diese Differenzierung schlägt sich in jeweils unterschiedlichen Erhebungsvoraussetzungen nieder, was nachfolgend anhand der in den Landesberichten untersuchten Aspekte verdeutlicht wird.

a) Allgemeine Erhebungsvoraussetzungen

Die Gegenüberstellung der allgemeinen Erhebungsvoraussetzungen zeigt, dass beide Rechtsordnungen die Erhebung von Geheimdienstinformationen an den Verhältnismäßigkeitsgrundsatz binden. Auffallend ist jedoch die unterschiedliche Annäherung an die Verhältnismäßigkeitsprüfung. Das amerikanische Recht sieht hierzu den Erlass sogenannter *minimization procedures* vor. Diese Regeln werden vom *Attorney General* individuell für die einzelnen Überwachungsmethoden erlassen und sollen einen angemessenen Ausgleich zwischen den verschiedenen widerstreitenden Interessen gewährleisten.

Im deutschen Recht müssen die einzelnen Ermächtigungsgrundlagen und Ermittlungen ebenfalls den Anforderungen des Verhältnismäßigkeitsgrundsatzes genügen. Dieses Erfordernis muss jedoch nicht zwingend ausdrücklich normiert sein. Vielmehr resultiert diese Vorgabe aus dem allgemeinen Gesetzesvorbehalt sowie dem verfassungsrechtlichen Bestimmtheits- und Verhältnismäßigkeitsgrundsatz und muss daher stets beachtet werden.

Die national unterschiedliche Herangehensweise führt in der praktischen Anwendung kaum zu Unterschieden. Die ausdrückliche Fixierung in den USA ist insofern nicht notwendigerweise mit einem höheren Schutzniveau verbunden. Zum einen steht die Entscheidung über den konkreten Methodeneinsatz im Ermessen der Dienste,[62] zum anderen werden bei ernsthaften Bedrohungen der nationalen Sicherheit selbst eingriffsintensive Maßnahmen gestattet.[63] Entgegen der ersten Vermutung gewährleisten die in den *minimization procedures* formalisierten Verhältnismäßigkeitskontrollen kein signifikant höheres Schutzniveau als die Vorgaben des deutschen Rechts.

b) Bedeutung des Beobachtungssubjekts

Als zweite Eigenheit erweist sich die unterschiedliche Berücksichtigung der Staatsangehörigkeit des Betroffenen. Während in den USA das Schutzniveau entsprechend den Vorgaben des vierten Verfassungszusatzes variieren kann, ist eine solche Differenzierung im deutschen Kontext nicht vorgesehen. Im amerikanischen Recht gelten beispielsweise bestimmte Erhebungsvoraussetzungen nur bei *U.S. Persons*. Dies gilt etwa für den Schutz der *minimization procedures* und den auf den ersten Verfassungszusatz gestützten Anwendungsausschluss. Dem deutschen Recht ist eine an Nationalitäten anknüpfende Unterscheidung weitgehend fremd und wird höchstens als Begründung für zusätzliche Schutzvorkehrungen herangezogen, wie etwa die Hinzuziehung eines Dolmetschers. Eine Ausnahme von dieser Grundregel bildet die strategische Überwachung im Ausland. Dort gestattet § 5 II 2, 3 G10 ausnahmsweise die Identifizierung von Telekommunikationsanschlüssen, sofern eine gezielte Erfassung von Anschlüssen deutscher Staatsangehöriger ausgeschlossen werden kann.

c) Einteilung der Ermittlungsmethoden

Eine dritte Besonderheit ist die unterschiedliche Kategorisierung der einzelnen Ermittlungsmethoden. In beiden Rechtsordnungen steigen zwar die Erhebungsvoraussetzungen mit zunehmender Eingriffsintensität, diese Abstufungen beruhen jedoch auf zum Teil unterschiedlichen Erwägungen. Während in Deutschland die Ermittlungsmethoden in Abhängigkeit von der Intensität des Grundrechtseingriffs eingeteilt werden, orientiert sich die Einstufung im amerikanischen Recht oftmals an den Vorgaben des vierten Verfassungszusatzes. Das deutsche Recht stuft daher andere Maßnahmen als geringfügig ein als das amerikanische Recht.

---

[62] Vgl. Mukasey Guidelines 2008 unter Punkt I.C.2.a.: "the choice of methods is a matter of judgment".

[63] Vgl. Mukasey Guidelines 2008 unter Punkt I.C.2.a "to use any lawful method […] even if intrusive, where the degree of instrusiveness is warranted in light of the seriousness of a criminal or national security threat".

Im deutschen Kontext umfassen die schlichten Erhebungsmaßnahmen zum Beispiel die offene Informationserhebung beziehungsweise die Erhebung aus offen zugänglichen Quellen und damit Maßnahmen ohne oder mit nur geringer Eingriffsintensität. Eingriffsintensivere Maßnahmen werden demgegenüber an strengere Voraussetzungen geknüpft. Der gezielt gegen bestimmte Personen gerichtete Einsatz von V-Männern muss sich beispielsweise an die verfassungsrechtlichen Rahmenbedingungen halten und damit unter anderem das Recht auf informationelle Selbstbestimmung und die Selbstbelastungsfreiheit beachten.[64] Eine völlig bedingungslose Infiltration ist nicht möglich, sondern erfordert nach § 9 II BVerfSchG zumindest das Vorliegen von Tatsachen für verfassungsfeindliche Bestrebungen i.S.d. § 3 I BVerfSchG.

Im amerikanischen Kontext werden demgegenüber entsprechend dem Verfassungsverständnis Maßnahmen der *threat assessment* als geringfügig eingestuft. Da diese mangels schutzwürdigen Vertrauens nicht von der Verfassungsgarantie erfasst werden, können öffentliche Einrichtungen und Organisationen trotz erheblicher Eingriffsintensität ohne Bindung an relevante Voraussetzungen infiltriert werden.[65]

d) Beispiel der Telekommunikationsüberwachung

Weitere Charakteristika des nationalen Geheimdienstrechts werden am Beispiel der nachrichtendienstlichen Telekommunikationsüberwachung deutlich.[66] Diese bietet sich als Vergleichsbeispiel an, da sie einheitlich von beiden Rechtsordnungen als besonders eingriffsintensive Form der Informationsgewinnung eingestuft wird. Die einschlägigen Ermächtigungsgrundlagen des G10 beziehungsweise des FISA unterscheiden sich in Bezug auf die Zielsetzung, die allgemeinen Schutzkonzepte und den Kernbereichsschutz.

aa) Abweichende Zielsetzung

Ein erster Unterschied resultiert aus der unterschiedlichen Zielsetzung beider Ermächtigungsgrundlagen. Im deutschen Recht darf der Primärzweck der nachrichtendienstlichen Telekommunikationsüberwachung nicht durch andere Verwendungsmöglichkeiten überlagert werden. Demgegenüber ist im amerikanischen Recht eine solche Einschränkung seit dem Umbau der Sicherheitsarchitektur nicht

---

[64] Zur grundsätzlichen Zulässigkeit vgl. BGH NStZ 1996, S. 450, sowie *Soiné,* NStZ 2010, S. 597, 599. Vgl. zur kriminalistischen List *Korte,* in: Korte/Zoller, S. 65f; *Soiné,* NStZ 2010, S. 596ff.

[65] Vertiefend *Berman*, S. 22.

[66] Allgemein zum Vergleich zwischen Deutschland und den USA siehe *Gitenstein,* in: Wittes, S. 30; *Scheppele,* Fordham L. Rev. (75) 2006, S. 621.

mehr vorhanden. Dort beansprucht der sogenannte *primary purpose*-Test seit den Reformen nach 2001 keine Geltung mehr. Nach diesem durften FISA-Erkenntnisse ursprünglich nur verwertet werden, wenn der „primäre" Zweck der Informationserhebung einen Auslandsbezug aufwies. In der aktuellen FISA-Fassung ist für eine Überwachung nunmehr ausreichend, dass der Erhalt von *foreign intelligence information* einen „wesentlichen" Zweck der Überwachung darstellt.

Eine Telekommunikationsüberwachung nach deutschem Recht ist demgegenüber an die Zielvorgabe des § 1 G10 gebunden, welche ihrerseits durch die höchstrichterliche Rechtsprechung eine umfassende inhaltliche Ausgestaltung erfahren hat. In dieser Hinsicht betonte das Bundesverfassungsgericht in seinem Urteil zur Fernmeldeüberwachung durch den BND, dass nur die Aufklärung internationaler Gefahrenlagen die Breite und Tiefe der Grundrechtseingriffe rechtfertige.[67] Dieses Urteil ist für den vorliegenden Rechtsvergleich von Interesse, da es eine an den *primary purpose*-Test erinnernde Formulierung benutzt. Nach den Worten des Bundesverfassungsgerichts müsse der Gesetzgeber „dafür Sorge tragen, daß die Ermächtigungen […] auf die Aufgaben des Bundesnachrichtendienstes bezogen bleiben und anderweitige Verwendungsmöglichkeiten die Primärfunktion nicht überlagern".[68] Die im deutschen Recht fortwährende Anknüpfung an den Primärzweck der Maßnahme erweist sich daher seit der Abschaffung des *primary purpose*-Tests als signifikanter Unterschied zum amerikanischen Modell.

bb) Abweichende Schutzkonzepte

Weitere Abweichungen ergeben sich in Bezug auf die jeweils geltenden Schutzkonzepte. Diese folgen in Deutschland den Vorgaben der klassischen Grundrechtsdogmatik, während in den USA die Garantien des ersten und vierten Verfassungszusatzes von Bedeutung sind.

In Deutschland unterliegen sämtliche Informationseingriffe den durch den Grundrechtskatalog gesetzten Grenzen. Der Schutzbereich der einzelnen Grundrechte wurde durch das Bundesverfassungsgericht stetig präzisiert und ausgeweitet. Im Bereich der Telekommunikationsüberwachung werden neben dem Kommunikationsinhalt unter anderem die Vertraulichkeit des Kommunikationsvorgangs, die informationelle Selbstbestimmung sowie die Integrität informationstechnischer Systeme geschützt. Besondere Schutzvorkehrungen sind zudem bei Vorgängen zu beachten, die dem Kernbereich privater Lebensgestaltung zugeordnet werden. Diese sind bei nachrichtendienstlichen Telekommunikationsüberwachungen ausdrücklich nach § 3a G10 zu berücksichtigen.

---

[67] BVerfG NJW 2000, S. 55, 65.

[68] Vgl. BVerfG 100, 313, 371f, 383, zur Telekommunikationsüberwachung des BND, sowie *Grunwald,* S. 123f.

Im FISA sind demgegenüber keine vergleichbaren Sonderregelungen vorhanden. Ein über die verfahrensrechtlichen Anforderungen hinausgehender Schutz von Individualrechten wird nicht für erforderlich gehalten, solange kein formelles Verfassungsrecht verletzt wurde.[69] Die im Verfahren bestehenden Beteiligungsrechte werden insofern als hinreichender Ausgleich betrachtet.[70] Im Vergleich zur deutschen Diskussion überrascht zudem die Rechtsprechung amerikanischer Gerichte, die verschiedene Vorgänge schrittweise dem Schutzbereich des vierten Verfassungszusatzes entzieht. Danach werden etwa Kommunikationsvorgänge mit Zustimmung des Anschlussinhabers *(consent-exception)*, Daten im Zugriffsbereich Dritter *(third-party exception)* sowie Nichtinhaltsdaten *(nonconsent exception)* nicht vom vierten Verfassungszusatz geschützt.[71] Als Argument wird vor allem das Fehlen eines schutzwürdigen Vertrauens oder der Verlust der Privatheit der Daten angeführt. Eine derartige ausdrückliche Herausnahme der genannten Aspekte ist im deutschen Verfassungsrecht nicht vorgesehen. Zwar ist auch in Deutschland der Zugriff auf Verbindungs- und Bestandsdaten leichter möglich als auf Inhaltsdaten. Dennoch werden die genannten Datenbestände in begrenztem Maße weiterhin vom verfassungsrechtlichen Schutz umfasst. Ebenso verhält es sich mit der *consent-exception*. Anders als im amerikanischen Modell scheidet ein Grundrechtseingriff nach dem deutschen Recht erst aus, wenn alle Beteiligten auf den Grundrechtsschutz verzichtet haben.[72]

5. Vergleich der Kontrollmechanismen

In beiden Rechtsordnungen ist das Geheimdienstwesen in einen komplexen Kontrollapparat eingebunden, der sowohl Kontrollen im Vorfeld als auch im Anschluss an eine Überwachungsmaßnahme vorsieht. Zudem war in beiden Ländern eine Verlagerung beziehungsweise Einschränkung der verschiedenen geheimdienstlichen Kontrollmechanismen erkennbar. Sowohl die beschriebene Entwicklung als auch die Kontrollsysteme werden in beiden Rechtsordnungen kritisiert.[73] Diese Kritik betrifft in Deutschland vor allem die parlamentarischen und gerichtlichen Kontrollgremien, während im amerikanischen Recht die bestehenden Spielräume der Exekutive gerügt werden.[74]

---

[69] So *Rogall,* in: Wolter, S. 137, demzufolge die Fernwirkung und die Ausnahmen von Verwertungsverboten indes auf einer Abwägung beruhen können.

[70] Vgl. *Rogall,* in: Wolter, S. 120, 136, der diesen Unterschied auf die formale Ausrichtung des amerikanischen Rechtsschutzes zurückführt. Ebenso *Trüg,* S. 451f.

[71] Vgl. *Schwartz,* Hastings L.J. (54) 2003, S. 776, 782.

[72] Vgl. BVerfG NJW 1992, S. 1875f; *Schwartz,* Hastings L.J. (54) 2003, S. 776.

[73] Vgl. hierzu *Schwartz,* Hastings L.J. (54) 2003, S. 793.

[74] Zur Missbrauchsanfälligkeit *Scheppele,* Fordham L. Rev. (75) 2006, S. 622f.

a) Präventive Kontrolle im Vergleich

Die Erkenntnisse des Rechtsvergleichs werden zunächst für die Kontrollen im Vorfeld einer geheimdienstlichen Überwachung dargestellt.

aa) Schwerpunkt der Vorabkontrollen

Im deutschen und amerikanischen Geheimdienstrecht wird die Präventivkontrolle überwiegend der Selbstregulierung der Dienste überlassen. Der Fokus liegt dementsprechend auf internen Mechanismen, während externe Kontrollinstanzen bereits aus Gründen der Geheimhaltung die Ausnahme bilden. Diese interne Regulierung erfolgt regelmäßig durch eine Normierung spezieller Antrags- oder Anordnungskompetenzen sowie die Einhaltung bestimmter Zustimmungserfordernisse.

Die externen Vorabkontrollen folgen in beiden Rechtsordnungen hingegen sehr unterschiedlichen Kriterien. Diese sind erneut den Vorgaben der jeweiligen Rechts- und Sicherheitsarchitektur geschuldet. Im deutschen Kontext wird die Kontrolldichte daher vor allem durch die Bedeutung des jeweils betroffenen Grundrechts und die Eingriffsintensität der jeweiligen Ermittlungsmethode bestimmt. Die Einschaltung externer Kontrollinstanzen wird primär bei Eingriffen in Art. 10, 13 GG und damit Maßnahmen nach dem G10 oder der akustischen Wohnraumüberwachung für notwendig erachtet. Die Kontrollaufgabe selbst wird bei der Wohnraumüberwachung durch den Richter, im Schutzbereich des Art. 10 GG durch die G10-Kommission übernommen. Die jeweiligen Standards gelten einheitlich und damit unabhängig vom jeweiligen Zweck der nachrichtendienstlichen Aufklärung.

Demgegenüber wird in den USA eine gerichtliche Vorabkontrolle lediglich bei Maßnahmen im Anwendungsbereich des vierten Verfassungszusatzes für notwendig gehalten. Die Zuständigkeit und die Intensität der Vorabkontrolle bestimmen sich dort nach dem Zweck der Maßnahme (DII oder FII) und dem betroffenen Personenkreis (*U.S. Person* oder *Non-U.S. Person*). Die Kontrolle der rein inlandsbezogenen Aufklärung unterliegt demgemäß erneut den klassischen Regeln des Strafverfolgungssektors und damit dem Richtervorbehalt. Lediglich im Bereich der auslandsbezogenen Aufklärung nach dem FISA wurde mit dem FISC ein spezielles Kontrollorgan errichtet.

bb) Existenz spezieller Kontrollgremien

Sowohl der FISC als auch die G10-Kommission sind spezielle Sondergremien, die bei der Präventivkontrolle geheimdienstlicher Ermittlungen eine zentrale Rolle spielen. Von diesem Berührungspunkt abgesehen überwiegen jedoch die Unterschiede beider Kontrollorgane.[75]

---

[75] Vertiefend zu dem Vergleich *Hörauf,* S. 350ff.

Eine erste Abweichung betrifft die personelle Zusammensetzung des Gremiums. Mit Ausnahme des Vorsitzenden müssen die Mitglieder der G10-Kommission nicht über die Befähigung zum Richteramt verfügen, während der FISC vollständig mit Richtern besetzt ist. Die unterschiedliche Profession wirkt sich allerdings kaum auf die Wahrnehmung der Kontrollaufgaben aus, da die Unabhängigkeit der einzelnen Mitglieder in beiden Rechtsordnungen durch den konkreten Benennungsvorgang hinreichend sichergestellt wird. Zudem sieht der FISA im Gegensatz zum G10-Verfahren einen Instanzenzug vor, innerhalb dessen die Anordnungen vor dem FISCR und dem *Supreme Court* angegriffen werden können. Dieser Rechtsweg ist ebenso wie im deutschen Nachrichtendienstrecht von der Mitteilung an den Betroffenen abhängig und kann daher in gleicher Weise faktisch umgangen werden.

Ein weiterer Unterschied betrifft den Zuständigkeitsbereich beider Gremien. Die G10-Kommission befasst sich thematisch ausschließlich mit Maßnahmen nach dem G10, also mit dem Bereich der Kommunikationsfreiheit. Im Vergleich dazu wird der FISC bei sämtlichen FISA-Anordnungen tätig, womit unter anderem Durchsuchungen und sonstige Überwachungsmaßnahmen erfasst werden. Dieses relativ weite Kontrollfeld wird umgekehrt durch den Auslandsbezug des FISA wieder verengt. Die Kontrolle des FISC erstreckt sich demnach ausschließlich auf auslandsbezogene Aufklärungsmaßnahmen nach dem FISA, während bei rein inlandsbezogenen Aufklärungsmaßnahmen der klassische Richtervorbehalt zur Anwendung kommt.

In zeitlicher Hinsicht kann der FISC zudem ausschließlich eine Vorabkontrolle vornehmen, wohingegen die G10-Kommission zusätzlich den gesamten Prozess der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten begleitet. Zusätzliche Abweichungen ergeben sich hinsichtlich des Umfangs der jeweiligen Prüfungskompetenz. Die G10-Kommission überprüft als unabhängige Instanz sowohl Zulässigkeit als auch Notwendigkeit von Beschränkungsmaßnahmen. Im Vergleich dazu ist der Kontrollrahmen des FISC viel kleiner. Die ohnehin schon niedrigen Standards werden bei *Non-U.S. Persons* noch weiter abgesenkt.[76] Bei einem Sachverhalt, bei dem nur ausländische Mächte eine Rolle spielen, wird zum Teil sogar vollständig auf eine Kontrolle durch den FISC verzichtet.

cc) Intensität der Vorabkontrollen

Auch die externen Kontrollmechanismen sind im Anwendungsbereich des FISA deutlich schwächer ausgebildet als im deutschen Recht. Dieser Unterschied ist beachtenswert, da gerade im Bereich der aktuell bedeutsamen Terroraufklärung primär der FISA als Ermächtigungsgrundlage herangezogen wird. Das deutsche Kontrollsystem weist zwar seinerseits verschiedene Lücken auf, im Anwendungsbereich des G10 unterliegen die einzelnen Maßnahmen jedoch einem komplexen

---

[76] So *Hall,* Wake Forest L. Rev. (41) 2006, S. 74.

und strikten Kontrollkonzept. Die amerikanischen Instanzen bleiben deutlich unter diesem Niveau.[77] Anders als bei der G10-Kommission werden die Kontrollanforderungen im Bereich des FISC im Vergleich zu sonstigen Maßnahmen nicht erhöht, sondern aus Gründen einer effektiven Aufklärung sogar abgesenkt.

b) Nachträgliche Kontrolle im Vergleich

In beiden Rechtsordnungen unterliegen die Geheimdienste zudem Kontrollen, die im Anschluss an eine Überwachung eingreifen. Diese nachträglichen Kontrollmöglichkeiten sind sowohl im amerikanischen als auch im deutschen Kontext an die Bedürfnisse des Geheimdienstsektors angepasst. In beiden Rechtsordnungen konnten in dieser Hinsicht Einschränkungen des nachträglichen Rechtsschutzes sowie die Existenz spezieller parlamentarischer Kontrollorgane ausgemacht werden.

aa) Nachträglicher Individualrechtsschutz

In beiden Rechtssystemen werden die individuellen Rechtsschutzmöglichkeiten durch reduzierte Benachrichtigungspflichten der Dienste abgeschwächt. Die konkreten Benachrichtigungsmodelle weichen in ihrer theoretischen Grundkonzeption jedoch voneinander ab. Im deutschen Recht ist etwa nach § 12 G10 von einer grundsätzlichen Mitteilungspflicht auszugehen, die ausnahmsweise aufgrund staatlicher Interessen hinausgezögert werden kann. Demgegenüber verfolgt der FISA den umgekehrten Ansatz, Mitteilungspflichten sind hier nur in Ausnahmefällen vorgesehen. In der praktischen Anwendung scheinen sich diese unterschiedlichen Ansätze allerdings kaum auszuwirken, da in Deutschland in tatsächlicher Hinsicht ebenfalls weitaus mehr Mitteilungen zurückgestellt als positiv beschieden werden.[78]

bb) Parlamentarische Kontrolle

Neben den individuellen Rechtsschutzmöglichkeiten sehen beide Rechtsordnungen nachträgliche parlamentarische Kontrollmechanismen vor, welche die Schwächen der gerichtlichen Kontrollen ausgleichen sollen.[79] Zu diesem Zweck wurden mit dem PKGr in Deutschland und den verschiedenen *Intelligence Committees* in den USA spezielle Kontrollorgane errichtet. Im amerikanischen Recht setzen diese Einrichtungen ihren Fokus vor allem auf Effektivitätserwägungen, während im deutschen Kontext neben der Effektivität vor allem die politische Kontrolle im Mittelpunkt steht. In beiden Rechtsordnungen sind die jeweiligen Kontrollgremien in

---

[77] Vgl. zu dieser Einschätzung ebenfalls *Hörauf,* S. 353.

[78] Vgl. BT-Drs. 17/4278, S. 5: 112 Mitteilungen gegenüber 238 Rückstellungen.

[79] Vertiefend zum Vergleich der Kontrollinstitute *Hörauf,* S. 354ff.

der Wahrnehmung ihrer Funktionen auf Angaben vonseiten des Geheimdienstsektors angewiesen. Im deutschen Recht kann dieser Mangel durch die strikte Präventiv- und Begleitkontrolle der G10-Kommission zumindest teilweise ausgeglichen werden. Dies ist in Bezug auf die Kontrolle des FISC nicht der Fall. Da der erhebliche Ausbau des amerikanischen Geheimdienstsektors aufseiten der Kontrollinstanzen also nicht nachvollzogen wurde, wirkt sich dieses Defizit weitaus gravierender als ein Demokratiedefizit aus als in Deutschland.[80]

6. Zwischenergebnis zu den geheimdienstlichen Besonderheiten

Die Besonderheiten des deutschen und amerikanischen Geheimdienstrechts spiegeln sich in der Art und Weise der Informationserhebung wider. Die Unterschiede betreffen sowohl den Umfang der Aufgabenwahrnehmung, die Anforderungen an den jeweiligen Methodeneinsatz als auch deren Durchsetzungsmöglichkeiten. Viele dieser Gegensätze sind auf systembedingte Besonderheiten der jeweiligen Sicherheitsarchitektur sowie abweichende individualrechtliche Schutzkonzepte zurückführbar. Für das deutsche Recht konnte dies vor allem anhand des Trennungsgebots, des Sicherheitsföderalismus, des Legalitätsprinzips, der Kommunikationsfreiheit und des Rechts auf informationelle Selbstbestimmung verdeutlicht werden. Im amerikanischen Recht sind demgegenüber die Verbürgungen und Ausnahmen des ersten und vierten Verfassungszusatzes prägend. Zudem wird in beiden Rechtsordnungen überwiegend von externen Vorabkontrollen abgesehen. Stattdessen werden interne Aufsichtsmaßnahmen, eigenständige Kontrollgremien sowie nachträgliche Parlamentskontrollen bevorzugt.

B. Vergleich allgemeiner Grenzen einer Informationsnutzung

Bei einer vergleichenden Gegenüberstellung der allgemeinen Grenzen einer Informationsnutzung zeigen sich zwischen dem deutschen und dem amerikanischen Lösungsansatz ebenfalls Abweichungen. Ein zentraler Grund für die unterschiedliche Ausgestaltung bildet abermals die abweichende Konzeption des deutschen und amerikanischen Sicherheits- und Geheimdienstwesens. Im deutschen Recht unterliegt die Informationsnutzung aufgrund der Vorgaben des Trennungsgebots und der Zweckänderung insgesamt strikteren Regeln als im amerikanischen Kontext. Zwar begründen auch diese keine unüberwindbaren Hindernisse, dennoch durchlaufen die Informationen einen viel engmaschigeren Selektionsprozess als vergleichbare Erkenntnisse im amerikanischen Recht. Stellt man diese beiden Ansätze nebeneinander, scheint das deutsche Konzept einen Mittelweg darzustellen,

---

[80] Vgl. hierzu insgesamt *Hörauf,* S. 342.

der sowohl einen vollständigen Erkenntnisaustausch als auch eine vollständige Informationsblockade verhindert. Die theoretischen Nutzungsbeschränkungen des deutschen Rechts werden in der praktischen Umsetzung allerdings nicht immer eingehalten.

Beim Vergleich der jeweiligen allgemeinen Grenzen kann entsprechend der Struktur der Landesberichte im Einzelnen zwischen systembedingten und individualrechtlichen Begrenzungen unterschieden werden.

1. Systembedingte Grenzen

Unter dem Stichwort der systembedingten Grenzen wurde der Einfluss der nationalen Sicherheitsarchitektur behandelt. Im deutschen Recht betreffen diese Gestaltungsvorgaben zunächst die Auswirkungen des Trennungsgebots, das sowohl die Informationserhebung als auch die Informationsnutzung beschränkt. Die im deutschen Landesbericht diskutierte Notwendigkeit eines Zufallsfundes soll einer gezielten Umgehung des Trennungsgebots entgegenwirken. Zudem fordert das Trennungsgebot eine Trennung der verschiedenen polizeilichen und geheimdienstlichen Datensätze. Diese Aufteilung darf zumindest theoretisch nicht durch einen permanenten und ungehinderten Datenaustausch umgangen werden. Dies wird beispielhaft an der organisatorischen Aufgliederung des GTAZ in die polizeiliche und nachrichtendienstliche Informations- und Analysestelle deutlich. Die Informationen dürfen weder durch den Einsatz von Zwangsbefugnissen noch gezielt zu Zwecken der Strafverfolgung erhoben werden. Inhaltlich wird eine ausufernde Übermittlung durch die Übermittlungsschwellen der Nachrichtendienstgesetze verhindert. Im amerikanischen Recht bestehen keine vergleichbaren Vorbehalte.

Die aus dem Trennungsgebot ableitbaren Nutzungsgrenzen finden im amerikanischen Recht keine Entsprechung. Mit der Einfügung des *significant purpose*-Standards in den FISA wurden hier selbst die einfachgesetzlichen Beschränkungen weitgehend aufgehoben. Es sind dementsprechend sowohl der Einsatz von Zwangsbefugnissen als auch die planmäßige Nutzung des FISA zulässig. Voraussetzung ist lediglich, dass die Strafverfolgung nicht den einzigen Zweck der Maßnahme bildet. Zudem soll durch den Aufbau der *information sharing environment* ein möglichst vollumfänglicher Informationsaustausch erreicht werden. Übermittlungsschwellen würden diesem Ziel zuwiderlaufen und sind im amerikanischen Recht daher aktuell nicht vorgesehen. Zwar wird auch im deutschen Recht eine Optimierung der Informationsflüsse angestrebt, dieser Prozess darf jedoch nur innerhalb des vom Trennungsgebot zugelassenen Rahmens erfolgen.

Im deutschen Recht wird die Informationsnutzung zudem durch die Gestaltungsvorgaben des Sicherheitsföderalismus geprägt. Aufgrund der systembedingten Aufteilung in präventive und repressive Aufgabenfelder ist eine Übermittlung aus dem Geheimdienst- an den Strafverfolgungssektor mit einer Zweckänderung verbunden.

In der Folge können die Geheimdienstinformationen nur unter den Voraussetzungen der Zweckänderung genutzt werden. Da in den USA eine solche Einteilung nicht existiert, sind vergleichbare Schranken weder vorgesehen noch notwendig. Zum einen dürfen mit dem FISA von vorneherein mehrere Zwecke verfolgt werden. Zum anderen kann das FBI selbst zwischen der nachrichtendienstlichen und polizeilichen Aufgabenwahrnehmung wechseln und damit fließend von der Wahrnehmung nachrichtendienstlicher Tätigkeiten in die Strafverfolgung übergehen. Anders als im deutschen Modell resultieren aus der Gestaltung der amerikanischen Sicherheitsarchitektur keine signifikanten Hindernisse, die einer Nutzung entgegenstehen.

2. Individualrechtliche Grenzen

Als weitere Schranke wurde der Einfluss von Individualrechten diskutiert. Beim Vergleich der Landesberichte wurde die unterschiedliche Gewichtung dieser Grenzlinie deutlich. In Deutschland existiert mit dem Recht auf informationelle Selbstbestimmung ein allgemeiner verfassungsrechtlicher Überbau der i.V.m. dem Gesetzesvorbehalt sämtliche Bereiche der Informationsnutzung erfasst.[81] Sowohl die staatliche Erhebung als auch die Speicherung und die Verwendung persönlicher Daten werden als Grundrechtseingriffe gewertet und sind daher zum Schutz des Einzelnen in ihrem Umfang zu beschränken. Dementsprechend müssen für die Informationserhebung, -verarbeitung und -übermittlung gesetzliche Grundlagen existieren, die den Anforderungen des Verhältnismäßigkeitsprinzips genügen. Bei der Nutzung von Geheimdienstinformationen wird dieses Prinzip durch den Aspekt der Zweckbindung und der Zweckänderung ergänzt. Die zur Einhaltung dieser Vorgaben geschaffenen Regelungen im BDSG, den Nachrichtendienstgesetzen und der Strafprozessordnung beschränken die Informationsnutzung sowohl aufseiten der Übermittlungs- als auch aufseiten der Empfangsbehörde.

Anders als im deutschen Recht wird dieser Bereich in den USA keiner umfassenden Regulierung zugeführt, sondern weitgehend der behördlichen Selbstregulierung überlassen. Zwar wird auch in der amerikanischen Verfassung der Schutz der Privatsphäre anerkannt,[82] während jedoch das deutsche Recht auf informationelle Selbstbestimmung außer auf die Privatheit der Daten auch auf den Zweck der Erhebung und den Verwendungszusammenhang abstellt, setzt das amerikanische Konzept der *privacy* an der Rechtmäßigkeit der Datenerhebung selbst an.[83] Das Vorliegen einer einseitigen Einwilligung, die Zugriffsmöglichkeiten Dritter oder das Fehlen eines objektiv schutzwürdigen Vertrauens lassen die Gewährleistungen des vierten Verfassungszusatzes entfallen. Der Schutz der Privatsphäre ist in den

---

[81] Vgl. *Weichert,* S. 13.

[82] Vgl. *Genz,* S. 39.

[83] Vgl. stellvertretend zum deutschen Recht *Weichert,* S. 17.

USA damit weitaus formaler ausgestaltet als im deutschen Recht. Ein allgemeines, für sämtliche Behörden auf Bundes- und Staatenebene geltendes Schutzkonzept oder inhaltliche Mindeststandards existieren nicht. Dieser Ansatz steht im krassen Gegensatz zu den vergleichsweise strikten Vorgaben des deutschen Rechts, welche die Erhebung, Verarbeitung und Nutzung der Daten umfassend regeln.

Die Auswirkungen der unterschiedlichen Schutzkonzepte auf die konkreten Nutzungsschranken werden zudem am Beispiel der Kommunikationsfreiheit deutlich.[84] Im deutschen Recht ist der Schutz der Kommunikationsfreiheit umfassend und entwicklungsoffen ausgestaltet.[85] Dieses in Anlehnung an das Recht auf informationelle Selbstbestimmung entwickelte Verständnis setzt der Erhebung und Verarbeitung der Daten weitaus striktere Grenzen als das amerikanische Recht. Während sich der Schutzbereich des Art. 10 GG sowohl auf den Kommunikationsinhalt als auch den Kommunikationsvorgang erstreckt, ist der Schutz des vierten Verfassungszusatzes primär auf Inhaltsdaten beschränkt.[86] Da bei Bestands- und Verbindungsdaten nach Ansicht der amerikanischen Rechtsprechung die erforderliche Privatheit fehlt, fallen diese nicht in den Anwendungsbereich des vierten Verfassungszusatzes. Dies ist im deutschen Recht anders. Dort werden Bestands-, Verbindungs- und Inhaltsdaten vom Grundrechtsschutz erfasst. Die unterschiedliche Schutzwürdigkeit wird erst bei der konkreten Ausgestaltung der erforderlichen Erhebungsstandards berücksichtigt.

C. Übermittlungsregeln im Vergleich

Die in Bezug auf die allgemeinen Nutzungsgrenzen festgestellten Unterschiede konnten für die im Geheimdienstrecht geltenden Übermittlungsstandards bestätigt werden. Auch bei diesen schlägt sich die unterschiedliche Gestaltung der Sicherheitsarchitektur in den nationalen Lösungsansätzen nieder. Diese betreffen sowohl die Akzeptanz eines Informationsaustausches als auch die generelle Existenz von Übermittlungsregeln. Während in Deutschland die Einfügung von limitierenden Übermittlungsvorschriften gesetzlich notwendig war, wird in den USA der Austausch von Geheimdienstinformationen sehr umfassend gestattet. Übereinstimmung besteht lediglich dahingehend, dass die amerikanischen und deutschen Strafverfolgungsbehörden bei schweren, staatsschutzrelevanten Sachverhalten in ähnlicher Weise auf das Wissen der Geheimdienste zurückgreifen können. Die unterschiedliche Gestaltung der Übermittlungsregeln wirkt sich daher erst unterhalb dieser Schwelle aus. Dies führt dazu, dass Geheimdienstinformationen im deutschen

---

[84] Vgl. bereits unter Teil 4, IV.A.4.

[85] Vgl. Maunz/Dürig-*Durner,* Art. 10 Rn. 47.

[86] Vgl. Maunz/Dürig-*Durner,* Art. 10 Rn. 60, 81; *Schwartz,* Hastings L.J. (54) 2003, S. 777.

Recht nicht zur Strafverfolgung einfacher Kriminalität übermittelt werden dürfen, während im amerikanischen Recht eine solche Differenzierung nicht erfolgt.

1. Akzeptanz eines Informationsaustausches

In beiden Rechtsordnungen dürfen die Geheimdienste Informationen an die Strafverfolgungsbehörden übermitteln. Die einzelnen Vorschriften sind im deutschen Kontext jedoch weitaus strikter und vor allem umstrittener als im amerikanischen Recht. In Deutschland sind die Verfassungsmäßigkeit, die Reichweite sowie das Verhältnis einzelner Übermittlungsvorschriften Gegenstand wissenschaftlicher und gerichtlicher Auseinandersetzungen. In diesem Zusammenhang wurde im deutschen Landesbericht unter anderem auf die Unstimmigkeiten zwischen den §§ 19, 20 BVerfSchG und § 161 I StPO verwiesen.

Demgegenüber werden in den USA die verschiedenen Übermittlungsmöglichkeiten höchstens in Bezug auf die Kompetenzaufteilung zwischen dem Bundes- und Einzelstaatenrecht diskutiert. Im amerikanischen Geheimdienstrecht ist zum Teil sogar eine Übermittlung von vorneherein entbehrlich, da die verschiedenen Behörden aufgrund gemeinsamer Datenbestände bereits über denselben Wissensstand verfügen.

2. Regelungsdichte der Übermittlungsregeln

Die beschriebenen Unterschiede in der Sicherheitsarchitektur schlagen sich folgerichtig in der generellen Häufigkeit von Übermittlungsregeln sowie deren Regelungsdichte nieder. Letztlich können in den USA geheimdienstliche Erkenntnisse für sämtliche Deliktsbereiche übermittelt werden. Ein derart umfänglicher Informationsaustausch scheitert in Deutschland an den Vorgaben des Trennungsgebots und der Zweckbindung.

In Deutschland wird eine Übermittlung zu Strafverfolgungszwecken aufgrund der Aufteilung in präventive und repressive Tätigkeitsfelder als erheblicher Grundrechtseingriff verstanden. Dieser kann nach Ansicht der Rechtsprechung nur bei Vorliegen einer hinreichend klaren und den Voraussetzungen der Zweckänderung genügenden Ermächtigungsgrundlage gerechtfertigt werden.[87] Die Vorschrift des § 20 BVerfSchG beschränkt die Übermittlung dementsprechend auf schwere beziehungsweise staatschutzrelevante Delikte. Im Bereich der besonders eingriffsintensiven Telekommunikationsüberwachung führen die noch strikteren Standards der §§ 4, 7 G10 daher auch nur zu einer geringen Zahl an Übermittlungen.

Im Gegensatz dazu zeichnet sich die Sicherheitsarchitektur der USA durch eine weitgehende Integration der verschiedenen Sicherheitsbehörden aus. Aus diesem

---

[87] Trotz der insofern unmissverständlichen Formulierung werden die Vorgaben von Teilen der Literatur allerdings missachtet.

Grund werden weder die Anfrageübermittlung noch die Eigeninitiativübermittlung problematisiert. Das amerikanische System geht insofern anders als das deutsche Recht von der grundsätzlichen Übermittelbarkeit der Daten aus. Lediglich in Bezug auf schwere Straftaten statuieren die Mukasey Guidelines eine Übermittlungspflicht, ohne diese jedoch durch einen Straftatkatalog näher zu präzisieren. Zudem werden in den USA zwar ebenfalls bestimmte Erhebungsbereiche besonderen Verfahrensregeln, etwa den *minimization procedures*, unterworfen. Diese sind jedoch nicht nur auf die Telekommunikationsüberwachung anzuwenden, sondern betreffen vor allem die Weitergabe von Erkenntnissen der auslandsbezogenen Überwachung nach dem FISA. Im Vergleich zu den Vorgaben des G10 und der Nachrichtendienstgesetze führen diese Regeln lediglich zu einer geringfügigen Beschränkung, da strafrechtlich relevante Sachverhalte überwiegend ausgenommen sind. Auf Daten von *Non-U.S. Persons* sind die Vorschriften zudem überhaupt nicht anwendbar und stehen einem Erkenntnisaustausch damit von vorneherein nicht entgegen.

D. Verwertungsregeln im Vergleich

Bei einer zusammenfassenden Betrachtung des deutschen und amerikanischen Verwertungsmodells wurden ebenfalls erhebliche Unterschiede deutlich. Während im deutschen Recht der Umfang der verwertbaren Erkenntnisse durch spezielle Verwendungsregeln bestimmt wird, unterliegen Geheimdienstinformationen in den USA den allgemeinen Regeln. Eine Begrenzung erfolgt dort jedoch über die generell strikteren Beweisstandards. Diese Grundstrukturen werden durch die nationalen Rechts- und Sicherheitsarchitekturen vorgezeichnet. Im deutschen Recht limitieren die Besonderheiten des Trennungsgebots, die Aufteilung in präventive und repressive Aufgabenfelder sowie das umfassende Recht auf informationelle Selbstbestimmung die in einem Strafverfahren nutzbaren Erkenntnisse. Vor ihrer eigentlichen Verwertung müssen Geheimdienstinformationen daher mehrere Hürden überwinden. Beginnend mit den Voraussetzungen der Übermittlungsschwellen über die Anforderungen der Zweckbindung und der Verwendungsregeln bis hin zu den klassischen Verwertungsverboten durchlaufen Geheimdienstinformationen mehrere Ausfilterungsprozesse. Der ursprüngliche Datenbestand wird dabei schrittweise reduziert, sodass nur ein geringer Anteil für eine beweisrechtliche Nutzung in Betracht kommt. Die im Strafverfahren letztlich zur Verfügung stehenden Informationen betreffen ausschließlich die in den Übermittlungsvorschriften genannten schweren Delikte, die üblicherweise dem Staatsschutzbereich entstammen. Zudem führen Fehler im Erhebungs- und Übermittlungsprozess bei einer Beteiligung der Geheimdienste regelmäßig zur Unverwertbarkeit der übermittelten Erkenntnisse.

In den USA unterliegen die Übermittlung, die Verwertung und die Fehlerfolgen aufgrund der weitgehend identischen Erhebungsstandards der verschiedenen

Sicherheitsbehörden keinen speziellen Vorgaben. Im Bereich der Auslandsaufklärung werden umgekehrt sogar die Annahme und der Nachweis eines Verwertungsverbots durch verschiedene Geheimschutzregeln erschwert. Eine dem deutschen Ansatz vergleichbare Tendenz existiert nicht. Die Unterschiede in der Sicherheitsarchitektur setzen sich damit auf Ebene der Beweisverwertung fort. Die Einzelheiten werden mithilfe der in den Landesberichten erzielten Erkenntnisse vertieft.

1. Existenz spezieller Verwertungsregeln

Bei vergleichenden Analysen kontinental-europäischer und anglo-amerikanischer Rechtskreise wird üblicherweise der unterschiedliche Kodifizierungsgrad beziehungsweise die abweichende Richterrolle betont.[88] Diese Differenzierung trifft bei einer Nutzung von Geheimdienstinformationen nur im Ausgangspunkt zu. Entsprechend der Zugehörigkeit des deutschen Rechts zum Gesetzesrecht wurde für den untersuchten Bereich mit § 161 II StPO eine spezielle Verwendungsregelung geschaffen. Die Einfügung dieser Vorschrift war notwendig, da bei einer Zweckänderung die Verwertungsbefugnis nicht bereits in der Erhebungsbefugnis enthalten ist und die Verwertung als grundrechtsrelevanter Vorgang aufgrund des Gesetzesvorbehalts einer Ermächtigungsgrundlage bedarf. Allerdings ist das in § 161 II StPO gewählte Konzept des hypothetischen Ersatzeingriffs seinerseits mit zahlreichen Unklarheiten behaftet, die eine künftige Präzisierung beziehungsweise Korrektur erwarten lassen.

In den USA sind spezielle Nutzungsregeln wiederum nur hinsichtlich der auslandsbezogenen Überwachung vorhanden. Diese Vorschriften beschränken sich zudem vorwiegend auf den Geheimschutz, ohne anderweitige Verwertungsstandards aufzustellen. Die Ausgestaltung der einzelnen Verwertungs- und Ausschlussregeln erfolgt dort zu weiten Teilen durch die Rechtsprechung.

2. Generelle Anforderungen

Bei einer Gegenüberstellung der herausgearbeiteten Grundstrukturen fällt auf, dass beide Rechtsordnungen die Verwertung zunächst nur für rechtmäßig erhobenes Datenmaterial vorsehen. Dem liegen jedoch unterschiedliche Ursachen zugrunde. In Deutschland beruht das Rechtmäßigkeitserfordernis auf dem umstrittenen Konzept des Zufallsfundes, das zur Wahrung des Trennungsgebots beitragen soll. In den USA resultiert dieses Erfordernis demgegenüber aus der formalen Ausrichtung des amerikanischen Beweisrechts. Nach dem Disziplinierungsgedanken sind die Ermittlungsbehörden zur Einhaltung der Erhebungsstandards angehalten, um eine Beweisverwertung nicht durch die Missachtung von Vorgaben zu gefährden.

---

[88] Vgl. zu diesem Vorurteil im Rahmen der Rechtsvergleichung *Brand,* JuS 2003, S. 1089.

Neben diesen unterschiedlichen Begründungsansätzen wird mit der Verwertungsproblematik auch insgesamt sehr unterschiedlich umgegangen. Aufgrund der Gestaltung der deutschen Sicherheitsarchitektur erfordert die Verwertung von Geheimdienstinformationen im deutschen Recht einen weitaus größeren Argumentationsaufwand als im amerikanischen Recht, das sehr angeglichene Sicherheitsstrukturen aufweist. In Deutschland erfolgt dementsprechend eine umfassende theoretische Aufarbeitung der Fragestellung.[89] Es wird versucht, die zweckändernde Datennutzung in die allgemeine Grundrechts- und Schrankendogmatik einzufügen. Die Grundrechtsrelevanz der Zweckänderung, die Vorgaben des Trennungsgebots und des Gesetzesvorbehalts zwingen den Gesetzgeber zu einer Regelung der wesentlichen Aspekte der Informationserhebung und -verarbeitung. Zudem definieren die Grundrechte den jeweils einschlägigen Schutzbereich und die möglichen Eingriffs- und Verwertungsschranken. Diese Vorgaben müssen bei der Ausgestaltung der maßgeblichen Ermächtigungsgrundlagen berücksichtigt werden, worauf sowohl Wissenschaft als auch Rechtsprechung vermehrt hinweisen. Trotz verschiedener Defizite haben diese Ansprüche damit zumindest zur Einfügung der beschriebenen allgemeinen und speziellen Verwendungsregeln in den Nachrichtendienstgesetzen und der Strafprozessordnung geführt.

In den USA wird die Verwertung geheimdienstlicher Erkenntnisse anders als im deutschen Recht keiner rechtlichen Sonderbehandlung zugeführt. Da die amerikanische Sicherheitsarchitektur nur noch geringfügig zwischen den einzelnen Ermittlungszweigen differenziert, wirkt sich die Beteiligung der Geheimdienste auf die Beweisverwertung kaum aus. Dies gilt seit 2001 sogar für Erkenntnisse der auslandsbezogenen Aufklärung, da durch den Verzicht auf die *wall* selbst FISA-Erkenntnisse einer nahezu vollständigen Nutzung zugänglich gemacht wurden. Beweisrechtlich regulierend wirken lediglich die klassischen Beweisregeln, die auch sonst zur Anwendung kommen. Da im amerikanischen System keine dem deutschen Recht vergleichbare Grundrechts- und Schrankendogmatik existiert, müssen die maßgeblichen Richtlinien vor allem den Verfassungsgarantien und der hierzu ergangenen Rechtsprechung entnommen werden.[90] Je nach Sachverhalt greifen damit unterschiedliche Maßstäbe, die stark durch die Rechtsprechung als Quasigesetzesrecht geprägt sind. Eine Bindung an klare Rechtfertigungsebenen oder spezielle Verwendungsregeln ist nicht vorgesehen. Ein unter Umständen bestehendes Schutzbedürfnis ist über die formell-rechtliche Ausgestaltung des Verfahrensgangs zu befriedigen. Zudem werden die bestehenden Verwertungsregeln bei einer Anwendung auf Geheimdienstinformationen erheblich von praktischen Erwägungen beeinflusst. Die strengen Regeln des amerikanischen Beweisrechts werden mit Blick auf die praktischen Bedürfnisse der geheimdienstlichen Informationsgewinnung aufgeweicht, was sich schließlich auch

---

[89] So bereits generell zu den Beweisverboten *Herrmann,* FS für Jescheck, S. 1291.

[90] Vgl. *Markwordt Skehan,* S. 434.

auf die Verwertbarkeit der Erkenntnisse auswirkt. So werden zum Beispiel Regeln wie die *hearsay rule* oder die *Miranda warnings* durch verschiedene Ausnahme- und Sonderregeln zugunsten einer Verwertbarkeit modifiziert.

3. Nutzung als Spurenansatz

Identische Lösungsansätze greifen wiederum bei der Heranziehung von Geheimdienstinformationen als Spurenansatz, welche in beiden Rechtsordnungen möglich ist. Diese Nutzungsbefugnis ist von erheblicher Relevanz, da geheimdienstliche Erkenntnisse hierdurch zumindest mittelbar einer strafrechtlichen Nutzung zugänglich gemacht werden können. Anders als in den USA ist dies im deutschen Recht aufgrund der besprochenen systembedingten und individualrechtlichen Nutzungsgrenzen erheblicher Kritik ausgesetzt.

4. Prüfungsmaßstäbe im Vergleich

An die Verwertung geheimdienstlicher Erkenntnisse werden entsprechend dem beschriebenen Grundverständnis abweichende Prüfungsmaßstäbe angelegt. Im deutschen Recht bestimmt das Institut des hypothetischen Ersatzeingriffs die einer unmittelbaren Verwertung zugänglichen Informationen. Im amerikanischen Recht existieren im Vergleich dazu keine speziellen Verwendungsregeln. Solange die formalen Erhebungsstandards eingehalten wurden, richtet sich die Beweisverwertung nach den Beweisregeln, die auch sonst im amerikanischen Recht zur Anwendung kommen. Ausgehend von diesen Unterschieden liegt dem deutschen Recht ein hypothetischer, dem amerikanischen Recht ein tatsächlicher Überprüfungsmaßstab zugrunde. Dies führt in aller Regel dazu, dass im amerikanischen Kontext geheimdienstliche Erkenntnisse sehr viel leichter als Beweismittel herangezogen werden können als nach deutschem Recht.

Im deutschen Modell sind im Einzelnen die Vorgaben des hypothetischen Ersatzeingriffs nach § 161 II StPO maßgeblich. Danach wird unter Zugrundelegung eines hypothetischen Sachverhalts untersucht, ob die Strafverfolgungsbehörden zur Vornahme einer vergleichbaren Ermittlungsmaßnahme ermächtigt gewesen wären. Die übermittelten Informationen müssen folglich den Rechtmäßigkeitserfordernissen sowohl des Geheimdienst- als auch des Strafverfolgungssektors genügen. Abseits des § 161 II StPO dürfen außerstrafprozessual erhobene Erkenntnisse nach § 161 I StPO nur verwertet werden, wenn sie aufgrund ihres Bagatellcharakters oder aus sonstigen Gründen keine beachtenswerte Grundrechtsrelevanz aufweisen. Dabei fließen der Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung als wesentliche Grundlagen der Verwertungsregeln in jede Inte-

ressens- und Güterabwägung mit ein.[91] Der Disziplinierungsgedanke spielt im deutschen Recht demgegenüber keine zentrale Rolle.[92]

In den USA liegt der Verwertung demgegenüber kein hypothetischer, sondern ein tatsächlicher Überprüfungsmaßstab zugrunde. Die Zulässigkeit des Beweismittels richtet sich nach der Ermächtigungsgrundlage, die der Erhebung originär zugrunde lag, wie zum Beispiel dem FISA. Die Voraussetzungen der hypothetisch greifenden Beweiserhebungsvorschriften sind irrelevant. Der Zusammenhang zur auslandsbezogenen Auslandsaufklärung spielt im amerikanischen Beweisrecht folglich keine Rolle, solange die Erkenntnisse selbst rechtmäßig erhoben wurden.[93] Diese Lösung ist aus deutscher Perspektive zunächst verwunderlich, da auch das amerikanische Recht in *Title III* vereinzelt strengere Voraussetzungen vorsieht. Obwohl der FISA somit Maßnahmen gestattet, die bei einer rein inlandsbezogenen Aufklärung nach *Title III* rechtswidrig wären, sind für eine Verwertung allein die Rechtmäßigkeitsvoraussetzungen des FISA maßgeblich. Dieser Fokus auf die ursprüngliche Rechtmäßigkeit fügt sich in die prozessrechtliche Ausrichtung der amerikanischen Verwertungsregeln ein.[94] Solange die Erhebungsmaßnahme selbst rechtmäßig und mit der Verfassung vereinbar ist, fehlt der für den Disziplinierungsgedanken und damit für die Annahme eines Verwertungsverbots erforderliche Anknüpfungspunkt. Eine separate Begrenzung der Verwertbarkeit unter materiellrechtlichen Erwägungen wird nicht für erforderlich gehalten. Das in diesem Zusammenhang zum Teil angeführte *right to privacy* ist in seinem Schutzumfang gerade nicht mit dem deutschen Schutz des Persönlichkeitsrechts vergleichbar.[95] Es ist weder inhaltlich noch seinem Umfang nach hinreichend klar definiert und spielt als Anknüpfungspunkt für ein Verwertungsverbot daher kaum eine Rolle. Die aus Gründen der Abschreckung erfolgende Annahme eines Verwertungsverbots kann dementsprechend auch nur mittelbar zum Schutz von Individualrechten beitragen. Der Beweisausschluss gleicht insofern nicht den Eingriff in die Privatsphäre aus, sondern versucht durch eine Sanktionierung derartige Verstöße lediglich in Zukunft zu verhindern.[96] Diese prozessuale Schwerpunktsetzung der Verwertungsregeln spiegelt sich auch in den Ausschlussgründen des *Title III* und des FISA wider. Der Beweisausschluss wird dort vor allem auf prozessuale Aspekte, wie den Erlass einer unzureichenden Durchführungsanordnung, einen Verstoß gegen die Anordnung selbst oder eine sonst rechtswidrige Durchführung der Maßnahme gestützt.

---

91 Vgl. *Herrmann,* FS für Jescheck, S. 1292f.

92 Vgl. *Rogall,* in: Wolter, S. 149.

93 Siehe *United States v. Ning Wen*, 471 F.3d 777, 778 (7th Cir. 2006): "there is no basis […] to reject evidence that was properly gathered". *Howell/Lesemann,* UCLA J. Int'l L. & For. Aff. (145) 2007, S. 153; *Kris/Wilson,* § 32:1, S. 279; *Vervaele,* Utrecht L. Rev. (1) 2005, S. 7.

94 Vertiefend zu den Beweisverboten *Herrmann,* FS für Jescheck, S. 1298.

95 So *Herrmann,* FS für Jescheck, S. 1298.

96 Vgl. *Herrmann,* FS für Jescheck, S. 1299ff; *Ossenberg,* S. 79f.

Die Intensität des Grundrechtseingriffs beim Betroffenen spielt insofern keine beachtenswerte Rolle. Im Anwendungsbereich des FISA können die Richter einen Verstoß gegen diese Vorgaben aufgrund der schwach ausgeprägten Prüfungskompetenz zudem nur in wenigen Fällen nachweisen. Die an die Verwertung von Geheimdienstinformationen anzulegenden Prüfungsmaßstäbe variieren damit erheblich.

5. Prüfungszeitpunkt im Vergleich

Die dargestellten Prüfungs- und Verwertungsregeln greifen zu jeweils unterschiedlichen Zeitpunkten. Allerdings sind in beiden Rechtsordnungen die Verfahrensabschnitte vor der eigentlichen Hauptverhandlung für den Ausgang des Strafverfahrens von erheblicher Bedeutung.

Im deutschen Recht sind die Voraussetzungen des hypothetischen Ersatzeingriffs bei der Entgegennahme der Informationen zu prüfen. Dementsprechend werden die Voraussetzung zunächst durch die Strafverfolgungsbehörden im Ermittlungsverfahren bei einer Heranziehung als Spurenansatz und später durch das Gericht im Rahmen der Hauptverhandlung bei der Verwendung zu Beweiszwecken untersucht. Sofern kein Anwendungsfall der Widerspruchslösung vorliegt, prüft das Gericht die Verwertbarkeit von Amts wegen.

In den USA werden die Zulässigkeitsfragen demgegenüber in den Verfahrensabschnitten vor der eigentlichen Hauptverhandlung geklärt. Hierdurch soll eine unsachgemäße Beeinflussung der Geschworenen verhindert werden. Der Betroffene muss daher bereits während des Vorverfahrens einen entsprechenden Antrag stellen.[97] Ein Verwertungsverbot kann er nur bei einer individuellen Betroffenheit geltendmachen. Dieses *standing*-Erfordernis weist Ähnlichkeiten zur deutschen Widerspruchslösung auf, deren Anwendungsbereich bei einer Nutzung von Geheimdienstinformationen allerdings noch weitgehend ungeklärt ist.

Die Zulässigkeit von Geheimdienstinformationen wird in beiden Rechtsordnungen letztlich zu unterschiedlichen Zeitpunkten diskutiert. Bei einer faktischen Betrachtungsweise sind die Unterschiede zum deutschen Recht jedoch weit weniger gravierend als zunächst erwartet. Im deutschen Recht wird zwar die Verwertbarkeit in der Hauptverhandlung geprüft, allerdings finden die nachrichtendienstlichen Erkenntnisse regelmäßig über die Strafverfolgungsbehörden und weniger durch eine direkte Übermittlung an das Gericht Eingang in das Strafverfahren. Da die Strafverfolgungsbehörden die übermittelten Geheimdienstinformationen in aller Regel durch eigene Ermittlungen und Einschätzungen anreichern, sind Defizite im Geheimdienstsektor in den Ermittlungsakten oftmals nicht mehr erkennbar oder korrigierbar. Diese Problematik wird zusätzlich durch die Übernahme exekutiver

---

[97] Vgl. Rule 12(b) FRCrimP.

Vorbeurteilungen durch den Richter verstärkt, sodass auch im deutschen Recht im Ermittlungsverfahren wesentliche Weichen für die Hauptverhandlung gestellt werden.[98]

6. Folgen von Fehlern im Vergleich

Neben den klassischen Verwertungsregeln wurden in den Landesberichten die beweisrechtlichen Folgen von Fehlern im geheimdienstlichen Erhebungs- und Übermittlungsprozess untersucht.

a) Anknüpfungspunkte für einen Beweisausschluss

Bei einem Vergleich der Landesberichte zeigen sich bezüglich der allgemeinen Verwertungsmodelle zunächst gewisse Ähnlichkeiten. In beiden Rechtsordnungen führt die bewusste Missachtung verfassungsrechtlicher Vorgaben zur Annahme eines Verwertungsverbots.[99] Umgekehrt wird bei anderen Fehlern die Unverwertbarkeit eines Beweismittels nur in Ausnahmefällen angenommen.[100] Diese beiden Extrempositionen haben die deutschen Strafgerichte mehrfach bestätigt.[101] Selbst im amerikanischen System wurde trotz der im Grundsatz strengen Ausschluss- und Fernwirkungsregeln der Ausnahmecharakter eines Beweisausschlusses Schritt für Schritt aufgeweicht.[102] Außer bei einer willkürlichen Missachtung von Verfassungsvorgaben führen Fehler im Erhebungs- und Verarbeitungsprozess weder im deutschen noch im amerikanischen Beweisrecht zu einem bedingungslosen Verwertungsverbot.

Abseits dieser Extremfälle behandeln beide Rechtsordnungen Fehler im Erhebungs- und Übermittlungsprozess sehr unterschiedlich. Die abweichenden Verwertungsmodelle beruhen zum einen auf den nationalen Beweisregeln, zum anderen sind sie abermals Ausdruck der unterschiedlichen Sicherheitsarchitektur. Eine Gegenüberstellung beider Landesberichte zeigt jedoch, dass beide Rechtsordnungen auf unterschiedlichen Wegen zu sehr ähnlichen Ergebnissen kommen. Dies beruht sowohl auf dem Charakter der in Staatsschutzsachen betroffenen Kriminalitätsfelder als auch der rechtlichen Konstruktion der Verwertungsregeln.

Diese Erkenntnis soll anhand der selbstständigen und unselbstständigen Verwertungsverbote nachvollzogen werden.

---

98 Vgl. *Schünemann,* GA 2008, S. 316f; *Rehbein,* S. 274.

99 So im Ergebnis *Ossenberg,* S. 183ff.

100 Vertiefend zu den ähnlichen Lösungsansätzen *Trüg,* S. 475ff, 484ff.

101 Vgl. stellvertretend für viele KK-*Senge,* Vor § 48 Fn. 27.

102 Vgl. *Ossenberg,* S. 91ff, 113, 183, die auf die Disponibilität des Disziplinierungszwecks verweist. Vertiefend *King,* Int'l Legal Persp. (12) 2002, S. 216f.

aa) Selbstständige Verwertungsverbote

Anders als im amerikanischen System ist das Institut der selbstständigen Verwertungsverbote im deutschen Recht von zentraler Bedeutung. Danach können im deutschen Verfahrensrecht Verwertungsverbote unabhängig von einem Verfahrensverstoß direkt aus den Grundrechten abgeleitet werden, sofern der Schutz des Grundrechts eine Unverwertbarkeit der Erkenntnisse gebietet. Insbesondere der Kernbereichsschutz ist als Grundlage eines selbstständigen Verwertungsverbots anerkannt.

Demgegenüber wird im amerikanischen Recht ein Beweisausschluss vor allem auf den Disziplinzierungsgedanken gestützt, sodass für die Bejahung eines Verwertungsverbots grundsätzlich ein Verfahrensverstoß erforderlich ist.[103] Solange die Ermittlungsbehörden formal rechtmäßig handeln, fehlt der für einen Beweisausschluss erforderliche Anknüpfungspunkt. Diese sollen im Grundsatz nicht materielle Grundrechtsverletzungen, sondern Verfahrensverstöße sanktionieren.[104] Die Annahme eines selbstständigen Beweisverwertungsverbots scheidet im amerikanischen Beweisrecht damit selbst bei kernbereichsrelevanten Vorgängen aus.[105]

Dieser Unterschied zum deutschen Lösungsansatz wirkt sich bei der Nutzung von Geheimdienstinformationen allerdings nur geringfügig aus. Die strengen Übermittlungsvorschriften der deutschen Nachrichtendienstgesetze reduzieren die zu Strafverfolgungszwecken übermittelbaren Erkenntnisse von vorneherein auf solche über schwerwiegende Delikte. Diese Kriminalitätsfelder werden durch die deutsche Rechtsprechungspraxis jedoch verschiedentlich dem unantastbaren Kernbereich entzogen und stattdessen einer abwägungsoffenen Schutzsphäre zugänglich gemacht.[106] Dementsprechend kann bei einer Nutzung von Geheimdienstinformationen auch im deutschen Recht der Kernbereichsschutz nicht immer gewährleistet werden. Damit fallen die Unterschiede bei der Nutzung kernbereichsrelevanter Geheimdienstinformationen deutlich geringer aus als zunächst erwartet. Eine eindeutige Aussage wird allerdings durch die Unvorhersehbarkeit der deutschen Rechtsprechungslösung erschwert.

bb) Unselbstständige Verwertungsverbote

Besondere Aufmerksamkeit ist zudem den unselbstständigen Verwertungsverboten zu schenken. Diese knüpfen die Unverwertbarkeit an die Verletzung einer

---

[103] So *Ossenberg,* S. 75ff. Die Integrität der Justiz oder der Schutz der Privatsphäre spielen bei der Begründung einer Ausschlussregel nur noch eine untergeordnete Rolle.

[104] Vgl. *Herrmann,* FS für Jescheck, S. 1298, 1302; *Rogall,* in: Wolter, S. 120.

[105] Vgl. *Rogall,* in: Wolter, S. 120, 137.

[106] Vgl. stellvertretend zu dieser Unterscheidung durch die Rechtsprechung *Roxin/Schünemann,* § 24 Rn. 55.

Beweiserhebungsvorschrift. Wie eingangs bereits festgestellt, führt ein derartiger Verstoß weder im deutschen noch im amerikanischen Recht zwingend zur Unverwertbarkeit des Beweismittels. Bei einer isolierten Betrachtung wäre zudem aufgrund der formalen Ausrichtung des amerikanischen Rechts tendenziell eine strengere Fehlerfolge zu erwarten als im deutschen Beweiswürdigungsmodell.[107]

Diese Erwartung kann hinsichtlich der Nutzung von Geheimdienstinformationen ebenfalls nicht bestätigt werden. Das in Deutschland praktizierte Regel-Ausnahme-Verhältnis wird bei einer Beteiligung der Geheimdienste aufgrund der Besonderheiten der Sicherheitsarchitektur und der insofern einschlägigen Verwendungsregeln ins Gegenteil verkehrt. Dementsprechend führen Fehler im geheimdienstlichen Erhebungs- oder Übermittlungsprozess mehrheitlich zur Annahme eines Verwertungsverbotes. Diese drastische Konsequenz wird bei einer Missachtung von Erhebungsvoraussetzungen unter anderem auf die zu unbestimmten Verwendungsregeln, die Begrenzung auf rechtmäßige Zufallsfunde oder überwiegende Individualinteressen gestützt. Bei Fehlern in der Informationsübermittlung wird die Unverwertbarkeit demgegenüber aus dem Charakter der Übermittlungsvorschriften als Verwendungsregeln gefolgert. Danach beschränken die Übermittlungsvorschriften die zulässige Nutzung von vorneherein auf bestimmte verhältnismäßige Zwecke, sodass außerhalb dieser Voraussetzungen eine Nutzung ausgeschlossen ist. Diese Erwägungen erklären zugleich, warum bei einer Beteiligung der Geheimdienste häufiger als sonst eine Fernwirkung bejaht wird. Die in Bezug auf Geheimdienstinformationen geltenden Fehlerfolgen sind damit, ebenso wie die Übermittlungs- und Zweckbindungsregeln, mittelbar auf die Gestaltung der deutschen Verfassungs- und Sicherheitsstruktur zurückführbar.

Im Gegensatz dazu löst der Erhalt rechtswidriger Geheimdienstinformationen in den USA keine vergleichbaren Automatismen aus. Vielmehr bestimmt sich die Verwertbarkeit anhand der auch sonst gültigen Beweisregeln. Die in der Rechtsprechung entwickelten Ausnahmen kommen bei der Nutzung von Geheimdienstinformationen in gleicher Weise zur Anwendung.[108] Abseits eines Verfassungsverstoßes ist ein Beweisausschluss sogar nur bei einer ausdrücklichen gesetzlichen oder richterlichen Anordnung notwendig. Ein solcher Beweisausschluss ist in den Ermächtigungen des FISA und des *Title III* bei einer Missachtung zentraler Erhebungsvorschriften vorgesehen. Dieses Merkmal erinnert an die Kriterien der deutschen Abwägungslösung, bei der unter anderem dem Gewicht des Verfahrensverstoßes eine zentrale Rolle bei der Beurteilung eines Verwertungsverbots zukommt. Von dieser Gemeinsamkeit abgesehen, unterscheiden sich die Fehlerfolgen ein-

---

[107] So etwa *King,* Int'l Legal Persp. (12) 2002, S. 217, 225.

[108] In diesem Sinne werden bestimmte Bereiche durch Konstruktionen wie der *reasonable expectation of privacy* oder der *third party exception* dem Anwendungsbereich des vierten Verfassungszusatzes entzogen und können damit von vorneherein keinen Verfahrensverstoß begründen.

fachgesetzlicher Verstöße erheblich. Im amerikanischen Recht kommt beispielsweise erneut die Unterscheidung zwischen Maßnahmen der *domestic intelligence* und der *foreign intelligence investigations* zum Tragen. Die Verwertungsregeln im Bereich der rein inlandsbezogenen Aufklärung sind weitaus strenger als bei auslandsbezogenen Konstellationen. Dieser Unterschied wurde im amerikanischen Landesbericht am Beispiel der Telekommunikationsüberwachung nach dem *Title III* und dem FISA dargelegt. Während im Rahmen des *Title III* die Beweiszulassung der vollumfänglichen richterlichen Kontrolle unterliegt, werden im FISA sowohl die richterliche Prüfungskompetenz als auch die Einwirkungsmöglichkeiten des Angeklagten erheblich eingeschränkt. Als Folge dieses verschärften FISA-Zulassungsverfahrens waren die amerikanischen Gerichte bislang nicht in der Lage, einen Verfahrensverstoß nachzuweisen. Seit der Öffnung des FISA für andere Überwachungsbereiche sind diese abgesenkten Standards für den Geheimdienstsektor zudem insgesamt prägend, sodass amerikanische Geheimdienstinformationen viel seltener einem Beweisausschluss unterliegen als vergleichbare Erkenntnisse im deutschen Kontext.

b) Mögliche Fehlerquellen

Ausgehend von den Unterschieden des deutschen und amerikanischen Geheimdienstwesens sind unterschiedliche Fehlerquellen denkbar. Da im amerikanischen Recht keine dem Trennungsgebot analoge Grenzziehung existiert, ist der gezielte Einsatz der Geheimdienste zur Erlangung von Beweismaterial anders als in Deutschland unschädlich. Solange die Anforderungen des *significant purpose*-Tests eingehalten wurden, steht der FISA einer Erhebung von Beweismaterial nicht entgegen. Um die Rechtmäßigkeit der Überwachungsmaßnahme und damit die Verwertbarkeit der Erkenntnisse zu ermöglichen, genügt jeder noch so geringe Konnex zur Auslandsaufklärung. Die im deutschen Beweisrecht zur Unverwertbarkeit führende bewusste Kompetenzüberschreitung ist in Bezug auf das amerikanische Sicherheitswesen damit selten denkbar.

Ähnliches zeigt eine vergleichende Betrachtung der Übermittlungsvorgänge. Da der Informationsaustausch im amerikanischen Recht kaum noch Grenzen unterliegt, sind rechtswidrige Übermittlungen kaum denkbar. In der amerikanischen Rechtsprechung ist insofern kein Fall bekannt, in dem die Unverwertbarkeit mit einem Fehler im Informationsaustausch begründet wurde. Im deutschen Kontext sind im Gegensatz dazu sowohl die Übermittlung als auch die Nutzung nachrichtendienstlicher Erkenntnisse sehr viel fehleranfälliger. Die Charakteristika der deutschen und amerikanischen Rechts- und Sicherheitsarchitektur beeinflussen dementsprechend zugleich die in beiden Geheimdienstsektoren möglichen Fehlerquellen.

c) Zwischenergebnis zu den Fehlerfolgen

Fehler werden im geheimdienstlichen Erhebungs- und Übermittlungsprozess in beiden Rechtsordnungen unterschiedlich behandelt. Während das deutsche Lösungsmodell durch die Existenz der Verwendungsregeln den Rahmen der zulässigen Zweckentfremdung vorgibt und damit ein Verstoß regelmäßig die Unverwertbarkeit der Geheimdienstinformation begründet, ist ein solcher Automatismus im amerikanischen Recht nicht vorgesehen. In beiden Rechtsordnungen können zwar Verfahrensfehler ein Verwertungsverbot beziehungsweise einen Beweisausschluss rechtfertigen, anders als die deutsche Rechtsprechungspraxis haben die amerikanischen Gerichte insbesondere in Bezug auf den FISA von dieser theoretischen Möglichkeit jedoch kaum Gebrauch gemacht. Letztlich ist der Verzicht auf die beweisrechtliche Nutzung fehlerhafter Geheimdienstinformationen im deutschen Recht wahrscheinlicher als im amerikanischen Kontext.

7. Hintergründe zu den Verwertungsregeln

Die Unterschiede im deutschen und amerikanischen Verwertungsmodell können auf verschiedene Aspekte zurückgeführt werden. Ein wesentlicher Grund für die im deutschen Recht bestehenden Verwendungsregeln liegt in den system- und grundrechtsbedingten Eigenheiten der deutschen Rechts- und Sicherheitsarchitektur. Diese haben ihren Niederschlag in den Vorgaben der Zweckänderung gefunden, welche eine unverhältnismäßige Verletzung des Rechts auf informationelle Selbstbestimmung sowie eine Umgehung des Trennungsgebots verhindern sollen. Das Institut des hypothetischen Ersatzeingriffs soll zudem der Verschmelzung präventiver und repressiver Aufgabenfelder entgegenwirken.[109]

Die abweichende Gestaltung der amerikanischen Sicherheitsarchitektur gibt umgekehrt den maßgeblichen Ausschlag für das amerikanische Lösungsmodell. Dem amerikanischen Sicherheitswesen ist eine Trennung zwischen Polizei und Geheimdiensten ebenso fremd wie eine Differenzierung zwischen präventiven und repressiven Aufgabenfeldern. Eine Übermittlung ist damit von vorneherein nicht mit einer Zweckänderung oder Umgehung von Erhebungsstandards verbunden. Zwar wird auch im amerikanischen Kontext zwischen der Erhebung von Beweismitteln i.S.v. *evidence* und der Erhebung von Geheimdienstinformationen i.S.v. *intelligence* unterschieden, hierbei handelt es sich jedoch nicht um eine zwischen den verschiedenen Behörden verlaufende Trennlinie. Anders als in Deutschland lassen sich die unterschiedlichen Erhebungsstandards nicht an einer organisatorischen Behördentrennung festmachen, sondern resultieren vor allem aus ermittlungstaktischen Erwägungen innerhalb ein und derselben Behörde. Die Erhebung von *intelligence* rechtfertigt in diesem Sinne zwar zunächst abgesenkte Standards, wird später

---

[109] Vgl. *Forkert-Hosser,* S. 37 Fn. 113; *Rehbein,* S. 234.

jedoch die Nutzung als Beweismittel angestrebt, sind die gesetzlichen Erhebungsvoraussetzungen unter Berücksichtigung der klassischen Beweisregeln einzuhalten. Schließlich lassen sich die Verwertungsmodelle zum Teil auf die unterschiedlichen Funktionen der Beweisverbote im jeweiligen Strafverfahren zurückführen.

Dieser Aspekt wurde bereits bei der vergleichenden Darstellung der Fehlerfolgen erörtert.[110] In diesem Zusammenhang könnte man zusätzlich versucht sein den abweichenden Wahrheitsbegriff als weiteren Begründungsansatz heranzuziehen. Bei einer Gegenüberstellung der vorliegenden Rechtskreise wird insofern oftmals auf den Kontrast zwischen der im amerikanischen Recht maßgeblichen Verfahrensgerechtigkeit beziehungsweise formellen Wahrheit und der im deutschen Recht maßgeblichen Ergebnisgerechtigkeit beziehungsweise materiellen Wahrheit verwiesen.[111] Bei der beweisrechtlichen Berücksichtigung der geheimdienstlichen Besonderheiten konnte dem Wahrheitsverständnis allerdings keine im Vergleich zu anderen Problemfällen herausgehobene Stellung zugesprochen werden. Zumal die Erzielung eines fairen Urteils ein Kernanliegen beider Verfahrensordnungen darstellt, erweist sich der Wahrheitsbegriff bezüglich der vorliegenden Problematik nicht als zentrales Unterscheidungskriterium.

V. Auswirkungen staatlicher Geheimhaltung

Die strafprozessuale Nutzung von Geheimdienstinformationen kann sowohl im deutschen als auch im amerikanischen Strafverfahren eine staatliche Zurückhaltung relevanter Erkenntnisse begründen. Als zentrale Rechtsgrundlagen einer Geheimhaltung konnten für das amerikanische Strafverfahren der CIPA und der FISA ausgemacht werden. Im deutschen Strafverfahren erweist sich wiederum die Abgabe einer Sperrerklärung nach § 96 StPO als zentrales Geheimhaltungsinstrument.

In beiden Rechtsordnungen wird versucht die mit einer Geheimhaltung einhergehenden Nachteile durch Kontroll- und Kompensationsmechanismen auszugleichen. Bei der Untersuchung konnten in diesem Zusammenhang bestimmte Geheimhaltungsstrategien ausgemacht werden, die im nationalen Recht jeweils vorrangig zur Anwendung kommen. Im amerikanischen Modell wird beispielsweise favorisiert, dass nur der Richter Einsicht in die Materialien erhält. Dieser kann vorab bestimmen, ob gesetzlich genau festgelegte Beweissurrogate den Geschworenen vorgelegt werden oder nicht. Gegebenenfalls kann er eine Nichtoffenlegung durch eine (Teil-)Einstellung sanktionieren. Im deutschen Modell verlagern sich die Kompensationsmechanismen demgegenüber auf die eigentliche Hauptverhandlung. In dieser kann der Richter durch die Möglichkeiten einer umfassenden Be-

---

[110] Siehe oben 4.

[111] Vgl. *Trüg,* S. 67, 69.

weissurrogation und der richterlichen Beweiswürdigung einen gerechten Ausgleich der widerstreitenden Interessen erzielen. Darüber hinaus finden sich im nationalen Recht weitere Geheimhaltungsstrategien, denen jedoch eine eher untergeordnete Bedeutung zukommt.

Die in den Landesberichten für die einzelnen Geheimhaltungsstrategien aufgedeckten Konflikte, Kontroll- und Kompensationsmechanismen sind Gegenstand der nachfolgenden Untersuchung.

A. Bestehende Interessens- und Rechtskonflikte

In beiden Rechtsordnungen schränkt die staatlich bedingte Geheimhaltung die Arbeit der für die Wahrheitsermittlung zuständigen Organe ein. Die Vorenthaltung strafrechtlich relevanter Erkenntnisse wird einmütig als beachtenswerte Beeinträchtigung der Wahrheitsfindung empfunden. Die in Geheimhaltungsfragen bestehenden Interessens- und Rechtskonflikte sind in beiden Ländern daher sehr ähnlich. Unabhängig vom nationalen Kontext werden vergleichbare Gründe und Grundsätze angeführt, die einer Geheimhaltung im Strafverfahren entgegenstehen. Die Nachteile für den Angeklagten sollen jeweils gering gehalten werden.

Die mit einer Geheimhaltung verbundenen Belastungen äußern sich entsprechend der nationalen Verfahrensstrukturen gegenüber unterschiedlichen Akteuren. Im deutschen Recht ist vor allem der Richter als Folge der richterlichen Aufklärungspflicht zur erschöpfenden Aufklärung des Sachverhalts verpflichtet. Diese Aufgabe kann er bei einer staatlich bedingten Geheimhaltung nicht in dem sonst üblichen Umfang wahrnehmen. In den USA erfolgt die Wahrheitsfindung demgegenüber mittels Haupt- und Kreuzverhör vor den Geschworenen.[112] Diese Art der Beweispräsentation und vor allem das im Parteiverfahren notwendige Wechselspiel werden bei einer Zurückhaltung verfahrensrelevanter Erkenntnisse ebenfalls in zentralen Bereichen beschnitten.

B. Regelungsdichte der Geheimschutzregeln

Die Ausgestaltung der Geheimhaltungsvorschriften ist in den beiden Ländern sehr unterschiedlich. Entgegen der klassischen Zuordnung des *Common* und *Civil Law* zum Fall- und Gesetzesrecht wird die Geheimhaltungsproblematik im amerikanischen Kontext einer viel differenzierteren Regelung zugeführt. Demgegenüber liegt im deutschen Recht der Schwerpunkt auf einer richterlich geprägten Beweis-

---

[112] Vgl. *Mahler,* S. 11; *Ossenberg,* S. 132.

würdigungslösung. Im Einzelnen muss zwischen den Geheimhaltungs-, Kompensations- und Beweiswürdigungsregeln unterschieden werden.

Unmittelbare Abweichungen werden bezüglich der Regelungsdichte der nationalen Geheimschutzregeln deutlich. In Deutschland existiert mit der Vorschrift des § 96 StPO eine relativ konzentrierte Gesetzesnorm, deren einzelne Tatbestandsmerkmale durch die akademische und richterliche Auseinandersetzung ausgebaut wurden. Dieser abstrakt-generellen Regelung steht in den USA ein eher pragmatischer Ansatz gegenüber. Dort werden zumindest für die *classification*-Entscheidungen mit den präsidialen *Executive Orders* für jede Legislaturperiode ausführliche und den aktuellen Sicherheitsbedürfnissen angepasste, untergesetzliche Vorgaben erlassen. Die damit verbundene Flexibilität kann in Deutschland lediglich über die Rechtsprechung erreicht werden, was im Vergleich zur amerikanischen Lösung jedoch weniger Transparenz bedeutet.

Dieser Unterschied setzt sich auf Ebene der Kompensationsregeln fort. Während der CIPA in Bezug auf die Surrogations- und Sanktionsmöglichkeiten spezielle Vorgaben für den Umgang mit geheimhaltungsbedürftigen Informationen vorsieht, kommen im deutschen Recht lediglich die klassischen Vorgaben der mittelbaren Beweisführung zur Anwendung.

In beiden Rechtsordnungen kaum reguliert ist wiederum der Aspekt der Beweiswürdigung. Weder das deutsche noch das amerikanische Recht präzisieren die bei einer staatlichen Geheimhaltung an die Beweiswürdigung zu stellenden Anforderungen. Lediglich im deutschen Recht wurden für diesen Bereich durch die Rechtsprechung die Institute der vorsichtigen beziehungsweise der hypothetischen Beweiswürdigung geschaffen. Im amerikanischen Kontext finden sich für die Geschworenen demgegenüber keine gesonderten oder vergleichbaren Instruktionen.

C. Wahrheits- und Verfahrensmodelle

Daneben können anhand der Geheimhaltungsproblematik die abweichenden Wahrheits- und Verfahrensmodelle beider Rechtsordnungen nachgezeichnet werden.[113] Allgemein wird dem deutschen Recht ein eher materielles Wahrheitsverständnis im Sinne einer Ergebnisgerechtigkeit zugrunde gelegt. Demnach erfolgt die Wahrheitsfindung grundsätzlich im Rahmen der Hauptverhandlung durch den Richter. Dem amerikanischen Recht wird hingegen ein formalisierter Wahrheitsbegriff im Sinne einer Verfahrensgerechtigkeit zugesprochen. Nach diesem Konzept wird der Sachverhalt wiederum vor allem durch die gleichmäßig verteilten, wechselseitigen Einflussmöglichkeiten der Parteien aufgeklärt. Diese theoretische Zuordnung der Verfahrensmodelle konnte für die Geheimhaltungsproblematik zumin-

[113] Vgl. allgemein zu dieser Thematik *Trüg,* S. 60ff.

dest teilweise bestätigt werden. Im deutschen Modell wurde deutlich, dass die mit der staatlichen Geheimhaltung verbundenen Nachteile vor allem durch den Einfluss des Richters in der Hauptverhandlung befriedigt werden sollen. Die infolge einer Sperrerklärung notwendige Ersetzung durch Beweissurrogate kann der Richter beispielsweise durch eine Herabstufung des Beweiswerts kompensieren. Bei einer Zurückhaltung entlastender Erkenntnisse muss er die staatlich verkürzte Beweisgrundlage dagegen durch eine fiktive Würdigung des hypothetischen Beweisergebnisses berücksichtigen. Diese und weitere Mechanismen sollen den Richter zur Ermittlung und Rekonstruktion der tatsächlichen Geschehensabläufe befähigen.

Im amerikanischen Recht werden im Gegensatz zum deutschen Modell die wesentlichen Unklarheiten und Surrogationsmöglichkeiten nicht durch die Geschworenen der Hauptverhandlung, sondern bereits im Vorfeld durch die Geheimhaltungsregeln des CIPA geklärt. In die Hauptverhandlung werden lediglich die nach dem CIPA vorsortierten, für die Verteidigung relevanten und ausreichend geschützten Erkenntnisse zugelassen. Der CIPA richtet sich insofern an alle Parteien des Strafverfahrens und soll theoretisch die bei einer Geheimhaltung verschobenen Gleichgewichte wiederherstellen. In dieser Funktion versucht er zugunsten einer fairen Verfahrensgestaltung sowohl eine unnötige Offenlegung irrelevanter geheimhaltungsbedürftiger Erkenntnisse als auch eine nicht notwendige Geheimhaltung erheblicher Erkenntnisse zu verhindern. Die letztlich zugelassenen Beweise beziehungsweise Surrogate können im Anschluss an die Zulassung von den Parteien im Wechselspiel vorgetragen werden und sind von den Geschworenen auf ihre Überzeugungskraft hin zu beurteilen.[114] Zwar dürfen die Geschworenen diese Beweise ebenfalls würdigen, eine zusätzliche Kompensation der Geheimhaltung oder ein hypothetischer Vergleich ist indes nicht vorgesehen. Die Mechanismen des CIPA und die darin vorgesehenen Beteiligungsrechte und Einwirkungsmöglichkeiten der Parteien werden als legitimes Mittel zur Herstellung von Gerechtigkeit erachtet und verkörpern demgemäß ein eher formalisiertes Wahrheitsverständnis.

In den Landesberichten sind Besonderheiten erkennbar, die der theoretischen Zuordnung beider Verfahrenssysteme widersprechen.[115] Unter Einbeziehung dieser Aspekte wird deutlich, dass die beschriebenen Wahrheitsbegriffe die Unterschiede der beiden Geheimhaltungsmodelle zwar in Teilbereichen erklären können, jedoch keines der Modelle diesen Vorgaben in vollem Umfang gerecht wird. So sind die im deutschen Modell vorgesehenen Mechanismen bei einer staatlichen Geheimhaltung nur bedingt zur Ermittlung des wahren Sachverhalts geeignet. Vor allem das Institut der hypothetischen Beweiswürdigung wird in seinen praktischen Auswir-

---

[114] Allgemein zum Wahrheitsverständnis in beiden Rechtsordnungen vgl. *Trüg,* S. 66ff; *King,* Int'l Legal Persp. (12) 2002, S. 187ff.

[115] Zudem ist bereits die Aufteilung in die unterschiedlichen Wahrheitskonzepte in ihrer Absolutheit nicht zutreffend.

kungen kritisiert. Dabei wird zum Teil bezweifelt, dass der Richter durch die Würdigung ihm unbekannter Entlastungsbeweise den tatsächlichen Sachverhalt ausreichend nachbilden könne. Die verfolgte Ergebnisgerechtigkeit könne durch eine fiktive Glaubwürdigkeitsbeurteilung eines nicht bekannten Zeugen nur schwerlich erreicht werden. In diesem Zusammenhang ist zu berücksichtigen, dass das deutsche Strafverfahren nicht allein durch die Hauptverhandlung, sondern auch durch die Vorgänge im Ermittlungsverfahren geprägt wird. Versäumnisse im Vorfeld können durch den Richter oftmals nicht mehr ausgeglichen werden, was sich nachteilig auf die materielle Wahrheitsfindung auswirken kann.

Vergleichbare Vorwürfe finden sich auch in Bezug auf das amerikanische Geheimhaltungsmodell. Den Vorschriften des CIPA beziehungsweise des FISA wird vorgeworfen, dass sie dem Angeklagten und seinem Verteidiger zahlreiche Einwirkungsmöglichkeiten versagen, die für eine effektive Verteidigung erforderlich wären. Das dem amerikanischen Modell zugrunde liegende Ziel der Verfahrensgerechtigkeit durch Waffengleichheit wird damit ebenfalls zugunsten der Exekutive unterlaufen.

D. Überblick über die verschiedenen Geheimhaltungsstrategien

Bei einer rechtsvergleichenden Gegenüberstellung der einzelnen Geheimhaltungsstrategien werden weitere Besonderheiten deutlich. Auffallend ist zunächst die abweichende Schwerpunktsetzung. Während in Deutschland eine vollständige Abschottung der geheimhaltungsbedürftigen Informationen favorisiert wird, steht im amerikanischen Recht die Strategie der Richterbeteiligung im Mittelpunkt. Die nachfolgenden Ausführungen widmen sich zunächst diesen Strategien, bevor im Anschluss auf die anderen Geheimhaltungsvarianten eingegangen wird. Den Abschluss bildet ein Vergleich der in Geheimhaltungsfragen zentralen Kontroll- und Kompensationsmodelle.

1. Vollständige Abschottung beziehungsweise Beteiligung des Richters

In den Landesberichten haben sich für das deutsche Recht eine vollständige Abschottung und für das amerikanische Recht eine Richterbeteiligung als zentrale Geheimhaltungsstrategien herauskristallisiert. Der nachfolgende Vergleich wird zeigen, dass den unterschiedlichen Lösungsmodellen beider Rechtsordnungen weitgehend identische Zielsetzungen und Wertungen zugrunde liegen. Die Wahl der jeweiligen Geheimhaltungsstrategie ist dabei vor allem den national abweichenden Verfahrensstrukturen geschuldet. Diese unterschiedlichen Hintergründe wirken sich auf die Voraussetzungen und Rechtsfolgen einer Geheimhaltung aus.

a) Hintergründe

Ausschlaggebend für die Wahl der unterschiedlichen Offenlegungs- und Geheimhaltungsregeln in geheimdienstrelevanten Strafverfahren sind sowohl die Eigenheiten des jeweiligen Sicherheitswesens als auch die unterschiedlichen Verfahrensstrukturen beider Rechtsordnungen.

Die in Deutschland und den USA unterschiedliche Verbindung der einzelnen Geheimdienst- und Sicherheitsbehörden wirkt sich auch auf die Zusammenarbeit mit dem Strafverfolgungssektor aus. Diese wiederum beeinflusst die Reichweite der jeweiligen Offenlegungspflichten. Das amerikanische Sicherheitswesen zeichnet sich in diesem Sinne durch eine weitgehende Verschmelzung geheimdienstlicher und polizeilicher Strukturen aus. In den USA werden die strafprozessualen Offenlegungspflichten daher zum Teil auf die Dienste ausgeweitet, um eine Benachteiligung des Angeklagten im Parteiverfahren zu vermeiden. Zur Erhaltung des notwendigen Geheimschutzes wurden im amerikanischen Recht der CIPA und der FISA geschaffen. Im Gegensatz dazu ermöglicht die in Deutschland bestehende Trennung der Sicherheitsbehörden eine komplette Abschottung des Geheimdienstsektors. Zwar sind die einzelnen Behörden dort ebenfalls zur gegenseitigen Amtshilfe verpflichtet, dieser Pflicht werden für die deutschen Dienste jedoch durch das Trennungsgebot Grenzen gesetzt. Um eine widerrechtliche Vereinigung polizeilicher und geheimdienstlicher Befugnisse zu verhindern, sind Anfragen daher von vorneherein nur hinsichtlich bereits vorhandener Erkenntnisse möglich. Zudem können die nachrichtendienstlichen Übermittlungsschwellen beziehungsweise -sperren einem Informationsaustausch entgegenstehen. Eine im Vergleich zum amerikanischen Recht mögliche Benachteiligung kann jedoch verhindert werden, da dem Betroffenen mit Einleitung des Ermittlungsverfahrens der staatliche Ermittlungsapparat zur Verfügung steht. Diese Unterstützung wird verfahrensrechtlich durch die staatsanwaltschaftlichen und richterlichen Ermittlungspflichten abgesichert.

Die in Geheimhaltungsfragen bestehende Schwerpunktsetzung ist weiterhin den abweichenden Strukturen des deutschen und amerikanischen Strafverfahrens geschuldet. Die auf einer Sperrerklärung basierende vollumfängliche Geheimhaltung unter gleichzeitiger Fortführung des Strafverfahrens auf der Grundlage mittelbarer Erkenntnisse ist im amerikanischen Recht nicht möglich. Anders als in Deutschland ist eine Beweissurrogation nach dem CIPA beziehungsweise dem FISA nur unter Einbeziehung des Richters vorgesehen. Bevor es daher zur Nutzung beziehungsweise Surrogation geheimhaltungsbedürftiger Informationen kommt, müssen diese Erkenntnisse zumindest dem Richter vorgelegt werden. Dieses im FISA und CIPA vorgesehene richterliche *in camera*-Verfahren scheint zunächst auf einen entscheidenden Unterschied beider Rechtsordnungen hinzuweisen. Bei einer funktionalen Betrachtung relativieren sich diese Gegensätze jedoch. Dabei ist der deutsche Richter nicht mit dem amerikanischen Richter, sondern mit den Geschwore-

nen gleichzusetzen. Insofern ist im amerikanischen Recht eine Einsicht in das belastende Beweismaterial allein durch die Geschworenen ebenso unzulässig wie eine dem Richter vorbehaltene Kenntnisnahme im deutschen Strafprozess. Der Angeklagte hat in diesem Zusammenhang einen Anspruch auf Zugang zu allen Beweismitteln, die den Geschworenen während des Verfahrens vorgelegt werden.[116] Die Zwischenschaltung des amerikanischen Richters dient lediglich dazu die Geschworenen vor einer unsachlichen Beeinflussung zu schützen. Legt man im Vergleich den Fokus auf das über die Schuldfrage entscheidende Gremium, erweist sich das *in camera*-Verfahren nicht als signifikanter Unterschied zwischen den nationalen Geheimhaltungsmodellen. Vielmehr soll weder im deutschen noch im amerikanischen Strafverfahren dasselbe Gremium sowohl über die Schuldfrage als auch die Geheimhaltung oder Surrogation belastenden Beweismaterials entscheiden dürfen, wenn die Verteidigung umgekehrt über die maßgeblichen Umstände in Unkenntnis bleibt. Die im deutschen Recht gegen das strafprozessuale *in camera*-Verfahren vorgebrachte Kritik ist auf das im amerikanischen Recht existierende *in camera*-Verfahren daher nicht übertragbar. Die unterschiedlichen Lösungsmodelle sind nicht Ausdruck eines höheren oder niedrigeren Rechtsschutzverständnisses, sondern resultieren aus der im amerikanischen Recht vorzufindenden Trennung zwischen Richter und Geschworenen.

b) Voraussetzungen einer Geheimhaltung

Abgesehen von der unterschiedlichen Schwerpunktsetzung sind in Bezug auf die jeweilige Geheimhaltungsstrategie weitere Unterschiede beziehungsweise Gemeinsamkeiten erkennbar. Diese betreffen unter anderem Zuständigkeit, Form, Zeitpunkt, Gegenstand und Grund einer Geheimhaltungsentscheidung.

aa) Zuständigkeitsverteilung

In beiden Rechtsordnungen wird die maßgebliche Entscheidungsbefugnis auf Instanzen außerhalb des Strafverfahrens übertragen. Der Verbleib der Information im Geheimdienstsektor wird insofern einheitlich von Vertretern der Geheimdienste auf der Grundlage geheimdienstlicher Vorschriften im konkreten Einzelfall entschieden. Die einschlägigen Regelungen finden sich für das amerikanische Recht unter anderem im FISA, während für das deutsche Recht die nachrichtendienstlichen Übermittlungssperren, wie etwa § 23 BVerfSchG, greifen.

Noch striktere Zuständigkeitsregeln gelten für die außerhalb des Geheimdienstsektors getroffenen Geheimhaltungsentscheidungen. Eine solche Möglichkeit wird in Deutschland über die Abgabe einer Sperrerklärung nach § 96 StPO sowie in den USA durch eine *classification*-Entscheidung nach der E.O. 13526 erreicht. Die

---

[116] Vgl. *Turner/Schulhofer,* S. 20.

Entscheidungsbefugnis liegt in beiden Fällen bei hochrangigen Vertretern der Exekutive. Dies ist konkret für die Sperrerklärung die oberste Dienstbehörde, bei einer *classification*-Entscheidung der Präsident, sein Stellvertreter oder andere Behördenleiter. Weiterhin muss die Geheimhaltungsentscheidung bestimmten Formerfordernissen genügen. In Deutschland etwa ist die ausdrückliche Abgabe einer Sperrerklärung erforderlich. Die bloße Vertraulichkeitsbitte genügt nicht. Ebenso verhält es sich im amerikanischen Recht, das eine offizielle *classification*-Entscheidung vorschreibt.

bb) Zeitpunkt der Geheimhaltungsentscheidung

Gemeinsamkeiten bestehen in Bezug auf den Zeitpunkt der Geheimhaltungsentscheidung. Im Regelfall wird die Geheimhaltung in beiden Rechtsordnungen bereits vor der Hauptverhandlung beschlossen. Diese zeitliche Verortung gilt sowohl für die Übermittlungssperre des § 23 BVerfSchG und die Sperrerklärung nach § 96 StPO im deutschen Recht als auch die *classification*-Entscheidung und die Überprüfung der Offenlegungspflichten nach dem FISA oder dem CIPA im amerikanischen Recht.

Eine nachträgliche Geheimhaltung ist nur im Ausnahmefall vorgesehen. Ein Beispiel für derartige Ausnahmen ist die Regelung des § 8 CIPA. Danach können selbst während des Prozesses bestimmte Aktenbestandteile entfernt oder Zeugenvernehmungen gestoppt werden. In Deutschland ist eine nachträgliche Sperrerklärung demgegenüber nur bei Zeugen sowie in Bezug auf Erkenntnisse möglich, die noch nicht Aktenbestandteile geworden sind.

cc) Tauglicher Geheimhaltungsgegenstand

Weitere Gemeinsamkeiten bestehen hinsichtlich der tauglichen Geheimhaltungsgegenstände. Diese sind in beiden Rechtsordnungen sehr umfassend reguliert. Sowohl das amerikanische als auch das deutsche Recht formulieren die Geheimschutzregeln zwar zunächst ausdrücklich in Bezug auf Schriftstücke, bei einem vergleichbaren Schutzbedürfnis werden diese Regelungen jedoch zusätzlich auf andere Informationsquellen ausgedehnt.[117] Voraussetzung ist jeweils das Bestehen einer gewissen Zugriffsmöglichkeit. Sowohl die *classification*-Entscheidung als auch die Sperrerklärung stellen hierzu auf ein Besitz- oder Gewahrsamsverhältnis der Regierung ab. Lediglich im Anwendungsbereich des FISA ist die Geheimhaltung auf FISA-Vorgänge beziehungsweise FISA-Anträge begrenzt.

---

[117] Zum CIPA vgl. etwa *Zabel/Benjamin,* S. 101.

dd) Tauglicher Geheimhaltungsgrund

Ein weiteres Vergleichskriterium ist das Bestehen eines tauglichen Geheimhaltungsgrundes. Ein solches wird in beiden Ländern bei einer Gefährdung hochrangiger staatlicher Schutzinteressen bejaht, sofern diese Bedrohung mit einer gewissen Wahrscheinlichkeit zu erwarten ist. Die im amerikanischen Recht normierten Geheimhaltungsgründe erscheinen jedoch viel umfassender und ausdifferenzierter als die stark konzentrierte Regelung des § 96 StPO. In der E.O. 13526 werden unter anderem die tauglichen Geheimhaltungskategorien sowie die möglichen Schranken einer Geheimhaltungseinstufung aufgezählt. Während zum Beispiel der Methodenschutz abseits des § 110b III StPO im deutschen Recht zum Teil sehr umstritten ist, wird er im amerikanischen Recht unproblematisch als Geheimhaltungsgrund anerkannt.[118] Da die Regelung des § 96 StPO jedoch durch die Rechtsprechung ebenfalls eine umfassende inhaltliche Präzisierung erfahren hat, können die Geheimhaltungsregeln bei der praktischen Anwendung vergleichbar flexibel gehandhabt werden. Die notwendige Flexibilität wird im amerikanischen Recht wiederum durch den allgemeinen Charakter der Regelungen erreicht.

Von dieser Gemeinsamkeit abgesehen, decken die einzelnen Geheimhaltungsgründe zum Teil jedoch unterschiedliche Schutzbereiche ab. Im deutschen Kontext stehen insofern der überindividuelle sowie der höchstpersönliche Rechtsgüterschutz im Vordergrund.[119] Sowohl die Übermittlungssperre nach § 23 BVerfSchG als auch die Sperrerklärung nach § 96 StPO erfassen daher neben staatsschutzspezifischen Gemeinwohl- und Sicherheitsbelangen zugleich Individualinteressen. In die Abwägungsentscheidung des § 96 StPO fließen folglich neben den staatlichen Geheimhaltungsinteressen und der Schwere der Straftat zusätzlich die für den Beschuldigten drohenden Nachteile einer Geheimhaltung sowie der Stellenwert des geheimhaltungsbedürftigen Beweismittels mit ein. Die *classification*-Entscheidung sieht zwar ebenfalls eine Abwägung unter Einbeziehung nationaler Sicherheitsinteressen vor, im Gegensatz zur Sperrerklärung handelt es sich jedoch nicht um eine Geheimhaltungsentscheidung im konkreten Einzelfall, sondern um die generelle Zuordnung einer Information zu einer bestimmten Geheimhaltungsstufe. Individualinteressen können daher zunächst nicht berücksichtigt werden. Die *classification* haftet erst einmal nur der Information selbst an, ohne dass ein Bezug zu einem konkreten Einzelfall besteht. Diese Entscheidung könnte man daher mit der im deutschen Recht möglichen Einstufung als Verschlusssache nach § 4 SÜG verglei-

---

[118] Dies gilt sowohl für die E.O. 13526 als auch den FISA. In der E.O. 13526 wird dies in der Aufzählung tauglicher *classification categories* unter Punkt 1.4. deutlich. Im FISA ergibt sich der Methodenschutz aus der Grundkonzeption des Gesetzes. Durch die Geheimhaltung von FISA-Vorgängen und Anträgen sollen nicht nur laufende Überwachungen, sondern es soll auch und vor allem der Methodenschutz gewährleistet werden.

[119] Vgl. vor allem *Lisken,* NJW 1991, S. 1658, 1660. Zur primär vorbeugenden und gefahrenabwehrenden Zielsetzung der Sperrerklärung siehe BGH NJW 1998, S. 3577f.

chen. Da die Abwägung im Rahmen der *classification*-Entscheidung anders als die Sperrerklärung auf die staatlichen Geheimschutz- und Strafverfolgungsinteressen begrenzt ist, wird zunächst eine potentiell umfassendere Geheimhaltung ermöglicht. Der konkrete Einzelfall- beziehungsweise Individualbezug wird im amerikanischen Recht erst durch den CIPA hergestellt. Dementsprechend kann auch erst nach Stellung eines entsprechenden CIPA-Antrags geklärt werden, ob die Regierung trotz der Geheimhaltungsbedürftigkeit zu einer Offenlegung verpflichtet werden sollte.

Getrennt zu beurteilen sind wiederum die im FISA geltenden Geheimhaltungsgründe. Anders als bei einer Sperrerklärung oder dem CIPA sehen diese Vorschriften eine Geheimhaltung nicht als Ausnahme, sondern als Regelfall vor. Sämtliche Erkenntnisse unterliegen danach der Geheimhaltung, sofern nicht der *Attorney General* ausnahmsweise eine Nutzung zur Strafverfolgung gestattet. Selbst wenn eine solche Erlaubnis vorliegt, werden lediglich die FISA-Erkenntnisse, nicht jedoch die der Überwachung zugrunde liegenden Vorgänge offengelegt. Letztere unterliegen aufgrund des Eingreifens des *Attorney General* regelmäßig der Geheimhaltung.[120]

c) Unmittelbare Rechtsfolgen einer Geheimhaltung

Ein letzter Vergleichsaspekt sind die an eine Geheimhaltungsentscheidung unmittelbar anknüpfenden Rechtsfolgen.

aa) Bindungswirkung der Geheimhaltungsentscheidung

Im Grundsatz gehen beide Rechtsordnungen von einer Bindungswirkung aus. Sowohl die *classification*-Entscheidung als auch die Sperrerklärung können durch die Gerichte zwar gerügt, nicht aber aufgehoben werden. Lediglich im deutschen Recht kann sich der Richter über eine willkürliche Sperrerklärung hinwegsetzen. Da das Gericht diese Absicht jedoch zuvor im Rahmen der Gegenvorstellung vorbringen wird, kann die Regierung die erforderliche Begründung regelmäßig nachbessern. Das Gericht wird in der Praxis daher nur selten einen Willkürfall nachweisen können.

Im Vergleich dazu sind die Einwirkungsmöglichkeiten des Richters nach dem CIPA sehr viel umfassender. Dieser kann unter Heranziehung der dort vorgesehenen Surrogations- und Sanktionsmöglichkeiten viel stärker korrigierend auf die Geheimhaltungsentscheidung einwirken als der deutsche Richter im Fall der Gegenvorstellung. Umgekehrt ist jedoch zu beachten, dass die Bindungswirkung das deutsche Gericht nicht an der anderweitigen Aufklärung des Sachverhalts hindert, während im amerikanischen Kontext als geheimhaltungsbedürftig eingestufte

---

[120] Dieser wird üblicherweise die Gefährdung der nationalen Sicherheit versichern.

Informationen ohne entsprechende Ermächtigung weder offengelegt noch genutzt werden dürfen. Dort kann selbst der Angeklagte mit einem Beweisausschluss belastet werden, wenn er die Nutzung von *classified information* nicht rechtzeitig anzeigt.

bb) Beweissurrogation und Sanktionsmöglichkeiten

Neben der Bindungswirkung ist eine Geheimhaltungsentscheidung mit weiteren, zum Teil abweichenden Konsequenzen verbunden. Während das deutsche Recht mit der vorsichtigen Beweiswürdigung eine umfassende Beweissurrogation ermöglicht, sind in den USA die tauglichen Beweissurrogate zum Schutz der Geschworenen gesetzlich bestimmt. Als Ausgleich stehen den amerikanischen Richtern jedoch sehr viel umfassendere Möglichkeiten zur Verfügung, eine ungerechtfertigte Geheimhaltung zu sanktionieren.

Im deutschen Strafverfahren führt die sperrbedingte Nichterreichbarkeit des sachnächsten Beweismittels im Regelfall zur Beweissurrogation und Beweiswürdigung durch das Strafgericht. In diesem Verfahrensabschnitt dürfen sämtliche erreichbaren Beweissurrogate herangezogen werden. Eine Verfahrenseinstellung ist demgegenüber nur in außergewöhnlichen Fällen vorgesehen. Ein solcher liegt nach Ansicht des BGH erst vor, wenn der Richter infolge der Geheimhaltung keine verantwortbare Überzeugung mehr bilden kann und dem Verfahren insgesamt die Grundlage entzogen wird.[121]

Der CIPA eröffnet ebenfalls die Möglichkeit, geheime Informationen durch Beweissurrogate zu ersetzen. Diese Entscheidung wird jedoch im Vorfeld durch den Richter getroffen. Dieser soll die Offenlegung irrelevanter, aber schutzwürdiger Informationen verhindern sowie eine sichere Nutzung notwendiger Erkenntnisse gewährleisten. Da in der Hauptverhandlung nicht er, sondern die Geschworenen das Urteil fällen, ist der Richter jedoch von vorneherein auf die gesetzlich vorgeschriebenen Beweissurrogate angewiesen. Diese sind so konzipiert, dass eine bewusste Irreführung der Entscheidungsfindung möglichst ausgeschlossen ist. Stellt der Richter die Relevanz eines Beweismittels fest und kommt die Regierung dem Offenlegungsbegehren nicht nach, so kann er dieses Verhalten zum Beispiel durch eine (Teil-)Verfahrenseinstellung oder Wahrunterstellung des Verteidigungsvorbringens sanktionieren. Von dieser Möglichkeit kann er bereits dann Gebrauch machen, wenn von der Geheimhaltung wesentliche Informationen zur Schuldfrage betroffen sind. Anders als im deutschen Recht ist diese Sanktionsmöglichkeit im CIPA ausdrücklich gesetzlich normiert. Allerdings wird von dieser Regel auch im amerikanischen Recht eine Ausnahme gemacht; etwa wenn die Regierung darlegen kann, dass eine Verfahrenseinstellung dem Gerechtigkeitsempfinden

---

[121] BGH NStZ 2004, S. 343, 345.

widersprechen würde. Für diesen Fall ist die Beeinträchtigung der Verfahrensfairness durch andere Mechanismen auszugleichen.

2. Sonstige Geheimhaltungsstrategien

Neben der vollständigen Geheimhaltung beziehungsweise einer Offenlegung ausschließlich vor dem Richter wurden in den Landesberichten weitere Geheimhaltungsstrategien untersucht. Hierbei wurde deutlich, dass der konkrete Umfang der Geheimhaltung sowohl bei einer Sperrerklärung als auch bei der Nutzung von *classified information* mehreren Abstufungen unterliegen kann. Im deutschen Recht ist ein solches Stufenmodell bereits unter Verhältnismäßigkeitsgesichtspunkten geboten. Danach darf eine Sperrerklärung nur dann zu einer vollständigen Sperrung führen, wenn dem staatlichen Schutzbedürfnis nicht durch andere Schutzvorkehrungen Rechnung getragen werden kann.[122] Im amerikanischen Recht sind die verschiedenen Geheimhaltungsstufen wiederum dem Bedürfnis nach einer möglichst fairen und effektiven Verteidigerbeteiligung geschuldet. In den nachfolgenden Abschnitten werden die verbliebenen Geheimhaltungsmöglichkeiten einander gegenübergestellt. Der Vergleich beschränkt sich dabei auf die in nationalen Sicherheitsfragen ausschlaggebenden Besonderheiten.

a) Verteidigerbeteiligung

Neben den bereits diskutierten Geheimhaltungsstrategien kann der Schutz geheimhaltungsbedürftiger Informationen durch den Ausschluss des Beschuldigten beziehungsweise Angeklagten vom Verfahren beziehungsweise bestimmten Verfahrensschritten bei gleichzeitiger Beteiligung seines Verteidigers erreicht werden.

aa) Vor der Hauptverhandlung

In der Phase vor der eigentlichen Hauptverhandlung sind die Beteiligungsrechte des Beschuldigten in beiden Rechtsordnungen eher schwach ausgeprägt.[123] Sowohl im deutschen als auch im amerikanischen Strafverfahren kann der Beschuldigte unter erleichterten Bedingungen ausgeschlossen werden.[124] Die vorgesehenen

---

[122] In diesem Zusammenhang scheidet lediglich eine ausdrücklich auf den Richter begrenzte Offenlegung aus.

[123] Vgl. zum deutschen Recht *Roxin/Schünemann,* § 40 Rn. 35.

[124] Die im deutschen Recht diskutierten faktischen Ausschlussmöglichkeiten der Verteidigung durch Umgehung von Benachrichtigungen sowie der Verzicht auf die Aufnahme in die Strafakten werden nachfolgend nicht berücksichtigt. Sie spiegeln weder den Grundcharakter des deutschen Geheimhaltungsmodells wider, noch bieten sie den Geheimdiensten einen ausreichenden Geheimschutz. Zudem entfalten sie spätestens in der Hauptverhandlung keine Schutzwirkung mehr.

Beteiligungsrechte verringern sich bei einer Involvierung nationaler Sicherheitsinteressen zusätzlich. Bei entscheidungserheblichen Vorgängen muss in beiden Rechtsordnungen jedoch zumindest der Verteidiger anwesend sein.

Im amerikanischen Strafverfahren ist die auf den Verteidiger beschränkte Offenlegung von größerer Relevanz als im deutschen Recht. Dort kann über den Erlass einer Schutzanordnung die Offenlegung geheimhaltungsbedürftiger Informationen insgesamt auf einen sicherheitsgeprüften Verteidiger begrenzt werden. In diesem Fall erhält der Verteidiger Zugriff auf Informationen, die im deutschen Strafverfahren unter Umständen aufgrund einer Sperrerklärung geheim bleiben.[125] Während das im deutschen Recht bestehende umfassende Akteneinsichtsrecht nach § 147 StPO bei einer vollständigen Sperrung ins Leere läuft, sind auf der Grundlage einer *protective order* Abstufungen möglich. Im Gegenzug darf der Verteidiger die geheimhaltungsbedürftigen Erkenntnisse allerdings nicht mit seinem Mandanten teilen. Dieses Verbot ist nicht unumstritten, da es das Verhältnis zum Mandanten belasten kann und die Beurteilung eines Beweismittels nicht immer möglich ist. In der Folge können bedeutsame Erkenntnisse vom Verteidiger übersehen werden und damit gänzlich unberücksichtigt bleiben. Trotz dieser Kritikpunkte sind die Verteidigungschancen des Beschuldigten durch die zusätzlichen Einwirkungsmöglichkeiten des Verteidigers höher als dies im deutschen Strafverfahren bei einer vollständigen Sperrung der Fall wäre. Fehlt es demgegenüber an einer umfänglichen Sperrerklärung, wird der Betroffene durch das im deutschen Recht bestehende Akteneinsichtsrecht nach § 147 StPO besser gestellt.

bb) Während der Hauptverhandlung

In beiden Rechtsordnungen sind die Beteiligungsrechte in der Hauptverhandlung sehr viel stärker ausgebaut als im Ermittlungsverfahren. Der Schutz nationaler Sicherheitsinteressen durch den Ausschluss des Angeklagten ist weder im amerikanischen noch im deutschen Recht vorgesehen. Während im deutschen Strafverfahren aus Gründen der Sachverhaltsaufklärung zumindest jedoch ein zeitlich begrenzter Ausschluss möglich ist, wird im amerikanischen Strafverfahren die Beteiligung des Angeklagten als unerlässlich erachtet. Dieser Unterschied beruht auf den unterschiedlichen Konzeptionen beider Verfahrensmodelle.

Das deutsche Strafverfahrensmodell ist eher paternalistisch geprägt. Die Verfahrensleitung und die Verantwortung für die Wahrheitsermittlung obliegen dem Rich-

---

[125] Wollte man im deutschen Recht einen fiktiven Parallelfall bilden, müsste man dem Verteidiger die Einsichtnahme in die gesperrten Informationen gestatten, sodass dieser eine Gegenvorstellung an die Exekutive übersenden und um eine Offenlegung bitten dürfte. Da jedoch gesperrte Akten nicht mit einem Verwertungsverbot belegt sind, könnten die gesperrten Erkenntnisse, anders als im amerikanischen Recht, nicht mehr geschützt werden.

ter.[126] In diesem Konzept kann im Ausnahmefall bei einem konkret gefährdeten Zeugen der Angeklagte im Rahmen der Hauptverhandlung zeitweise von der Vernehmung ausgeschlossen werden. Dieser Ausschluss ist etwa gerechtfertigt, wenn eine drohende Sperrerklärung den Verlust eines Beweismittels begründen und damit die Wahrheitsfindung i.S.d. § 247 StPO beeinträchtigen würde. Da diese Ausschlussmöglichkeit jedoch primär der Sachverhaltsaufklärung und nicht dem Schutz nationaler Sicherheitsinteressen dient,[127] muss der Angeklagte unmittelbar im Anschluss an seine Zulassung umfassend über das Gesagte unterrichtet werden.

Im amerikanischen Modell ist demgegenüber ein formalisiertes Gerechtigkeitsverständnis vorherrschend, welches die Eigenverantwortlichkeit und Subjektstellung der Parteien stärker betont.[128] In diesem Modell ist der Ausschluss des Angeklagten von vorneherein unzulässig. Zwar kann die staatliche Geheimhaltung im Vorverfahren faktisch bis in die Hauptverhandlung fortwirken, letztlich sind jedoch nur die Erkenntnisse verwertbar, die dem Angeklagten und den Geschworenen unmittelbar vorgelegt werden.

b) Ausschluss der Geschworenen

Im amerikanischen Landesbericht wurde zudem der Ausschluss der Geschworenen bei gleichzeitiger Zulassung der anderen Verfahrensbeteiligten diskutiert.[129] Für diese Konstellation findet sich im deutschen Kontext keine Entsprechung. Bei der Bildung eines fiktiven Parallelfalls müsste als funktionales Äquivalent der deutsche Strafrichter über bestimmte Details in Unkenntnis bleiben. Eine derartige Geheimhaltungskonstellation ist im deutschen Strafverfahren weder sinnvoll noch notwendig. Während die Geschworenen als Laiengremium zum Teil vor irreführenden Informationen geschützt werden müssen, sind solche Schutzvorkehrungen beim deutschen Strafrichter aufgrund seiner Fachkompetenz nicht erforderlich.

Der Unterschied beider Verfahrens- und damit Geheimhaltungsmodelle kann beispielhaft anhand der im amerikanischen Recht für diese Konstellation vorgesehenen Präklusionswirkung des § 5 CIPA verdeutlicht werden. Danach kann die verspätete Mitteilung des Verteidigers zu einem vollständigen Ausschluss der *classified information* führen. Der Angeklagte soll die Geschworenen nicht durch die überraschende Einführung von geheimhaltungsbedürftigen Informationen in un-

---

[126] Vertiefend zu den philosophischen Grundlagen des inquisitorischen und adversatorischen Systems *King,* Int'l Legal Persp. (12) 2002, S. 194. Dieser bezeichnet den Staat als primären Akteur und den Einzelnen als primären „Empfänger" der staatlichen Aktivität.

[127] So *Weigend,* DJT, C 53.

[128] Vgl. *Feeney/Herrmann,* S. 353f; *King,* Int'l Legal Persp. (12) 2002, S. 193ff.

[129] Diese Ausschlussmöglichkeit ist nicht mit einem *in camera*-Verfahren zu verwechseln. Während die Einsicht *in camera* die auf bestimmte Personen begrenzte Offenlegung beschreibt, geht es vorliegend um die Geheimhaltung vor bestimmten Personen.

rechtmäßiger Weise beeinflussen können. Im deutschen Strafverfahren ist demgegenüber vor allem der Richter für die erschöpfende Sachverhaltsaufklärung zuständig, um auf dieser Grundlage ein materiell gerechtes Urteil erzielen zu können. Dementsprechend sind im deutschen Recht keine dem CIPA vergleichbaren Ausschlussfristen vorgesehen.[130] In § 246 I StPO wird sogar ausdrücklich klargestellt, dass ein Beweismittel nicht wegen einer verspäteten Vorbringung abgelehnt werden darf.[131] Zudem dürfte dem Angeklagten das Verhalten seines Verteidigers nicht zugerechnet werden, wenn ihn selbst kein Verschulden trifft.[132] Eine derartige Beschränkung würde den Angeklagten nicht nur erheblich belasten, sondern zugleich dem Amtsermittlungsgrundsatz zuwiderlaufen.

c) Ausschluss der Öffentlichkeit

Die Strategie des Öffentlichkeitsausschlusses ist sowohl im deutschen als auch im amerikanischen Strafverfahren vorgesehen. Anders als in Deutschland wurde dieser Bereich im amerikanischen Recht jedoch keiner Regulierung zugeführt, sondern primär der höchstrichterlichen Ausgestaltung überlassen. Die gerichtlich anerkannten Geheimhaltungsmöglichkeiten entsprechen weitgehend den Vorgaben, die auch das deutsche Recht vorsieht. Markante Besonderheiten sind, abgesehen von den Spezialregelungen im Bereich der Militärkommissionen, nicht erkennbar.

3. Zentrale Kontroll- und Kompensationsmechanismen

Den einzelnen Geheimhaltungsmöglichkeiten stehen verschiedene Kontroll- und Kompensationsmechanismen gegenüber. Sowohl das deutsche als auch das amerikanische Recht versuchen das durch die staatliche Geheimhaltung bewirkte Ungleichgewicht durch verschiedene Kontrollmechanismen, Surrogations- und Sanktionsmöglichkeiten beziehungsweise Beweiswürdigungslösungen auszugleichen.

a) Kompensation durch Kontrolle

Ein erster Kompensationsmechanismus wird in beiden Rechtsordnungen in der Schaffung interner wie externer Kontrollen gesehen. Diese können sowohl während als auch im Anschluss an das Verfahren greifen. Aus Gründen der Übersichtlichkeit werden die Kontrollen getrennt für die Informationsgewinnung und die Geheimhaltungsentscheidung untersucht.

---

130 Vgl. hierzu *Perron,* Beweisantragsrecht, S. 84f, 451.

131 Vgl. *Perron,* Beweisantragsrecht, S. 84f, 451. Ebenso die insofern übertragbare Rechtsprechung des Bundesverfassungsgerichts in BVerfG StV 1992, S. 307.

132 Vgl. *Perron,* Beweisantragsrecht, S. 91. Vgl. BVerfG NJW 1991, S. 351, zum Fristversäumnis.

aa) Kontrolle der Informationsgewinnung

Im deutschen Recht können geheimdienstliche Überwachungsmaßnahmen durch die Gerichte vollständig auf ihre Rechtmäßigkeit hin kontrolliert werden. Bei einer nachrichtendienstlichen Informationsgewinnung werden insofern weder ein Beurteilungsspielraum noch sonstige Einschränkungen der gerichtlichen Kontrollkompetenzen anerkannt.[133] In der Praxis können diese allerdings nicht immer in vollem Umfang ausgeschöpft werden. Zum einen kann sich eine Sperrerklärung auf relevante Zusatzinformationen beziehen, die für die Beurteilung der Rechtmäßigkeit der Überwachungsmaßnahme erforderlich sind. Zum anderen werden die deutschen Richter nicht immer über den erforderlichen Informationszugang verfügen, um den Diensten ein rechtswidriges Handeln nachweisen zu können.

In den USA richten sich Kontrollen demgegenüber vor allem nach den Regeln des CIPA und des FISA. Der CIPA selbst sieht unmittelbar keine Rechtmäßigkeitskontrolle der Überwachungsmaßnahme vor. Vor einer Beweiszulassung muss allerdings auch nach dem CIPA eine Relevanzprüfung durchlaufen werden, wodurch die Überwachungsmaßnahme zumindest indirekt auf ihre Rechtmäßigkeit hin untersucht werden kann. Diese richterliche Kontrolle unterliegt, ebenso wie im deutschen Recht, keinen rechtlichen Beschränkungen.[134] Der CIPA erreicht damit ein dem deutschen Modell vergleichbares Kompensationsniveau.

Dieses Ergebnis gilt nicht für die Kontrollen im Rahmen des FISA. Bei der Nutzung von FISA-Erkenntnissen sind sowohl die Prüfungskompetenz des Strafrichters als auch die Rügemöglichkeiten der Verteidigung schwach ausgebildet. Dies wird durch die tatsächlichen Gegebenheiten einer FISA-Überwachung zusätzlich verstärkt. Die für eine Rechtmäßigkeitsbeurteilung erforderlichen Informationen sind zwar mit Hilfe der *Brady Rule* zugänglich, die zu sichtenden Datenmengen können allerdings bei einer FISA-Überwachung einen nicht mehr überschaubaren Umfang erreichen. Während im deutschen Kontext das Strafgericht eine nach allen Seiten offene Aufklärungspflicht trifft, ist der Angeklagte im amerikanischen Parteiverfahren weitgehend auf sich allein gestellt. An dieser Schlechterstellung kann selbst eine durch die amerikanischen Gerichte gewährte Fristverlängerung nur geringfügig etwas ändern.

bb) Kontrolle der Geheimhaltungsentscheidung

Weitere Besonderheiten ergeben sich bezüglich der Kontrolle der Geheimhaltungsentscheidung. Hierbei ist zwischen internen und externen Kontrollen zu differenzieren.

---

[133] Vgl. Teil 1, III.4.c) sowie *Rehbein,* S. 185ff.

[134] Zudem greifen auch außergerichtliche Kontrollmechanismen. Im fünften Teil der E.O. 13526 sind periodische Rechtmäßigkeitskontrollen und Abstufungsmöglichkeiten der *classification*-Entscheidung vorgesehen, die sog. *review* und *declassification.*

(1) Interne Kontrollmechanismen

Die internen Kontrollmechanismen sind im deutschen und amerikanischen Recht sehr unterschiedlich ausgestaltet. Im deutschen Recht existieren für die behördliche Geheimhaltungsentscheidung, trotz der beschriebenen Fehleranfälligkeit, keine speziellen Kontrollmechanismen. Im Vergleich dazu finden sich in der E.O. 13526 mit der *review* und *declassification* formalisierte, interne Kontrollen, durch welche die Geheimhaltungseinstufung in regelmäßigen Zeitabschnitten auf ihre Korrektheit untersucht wird. Diese beiden Modelle sind hinsichtlich ihrer Kompensationswirkung allerdings nicht wirklich miteinander vergleichbar. Während der Sperrerklärung eine Abwägung unter Einbeziehung der widerstreitenden Gemein- und Individualinteressen zugrunde liegt, fehlt bei einer *classification*-Entscheidung dieser Einzelfallbezug. Die Verknüpfung zwischen staatlichem Geheimhaltungsinteresse und den Interessen des Angeklagten wird im amerikanischen Kontext erst durch die FISA- beziehungsweise CIPA-Kontrolle hergestellt. Die kompensatorische Wirkung der Geheimhaltungsentscheidungen kann daher nur zusammen mit diesen Kontrollmechanismen beurteilt werden. In einem zweiten Schritt sind daher vor allem die extern vorgesehenen Kontrollmöglichkeiten von Interesse.

(2) Externe Kontrollmechanismen

Bei der externen Kontrolle der Geheimhaltungsentscheidung muss zwischen den Kontrollen durch das Strafgericht und den sonst zwischengeschalteten Kontrollmöglichkeiten unterschieden werden.

Innerhalb des Strafverfahrens kann die Sperrerklärung im deutschen Recht nur bedingt auf ihre Rechtmäßigkeit kontrolliert werden. Die Strafrichter dürfen bei der Beurteilung der Geheimhaltungsentscheidung lediglich eine Plausibilitätskontrolle vornehmen und sind damit in ihrer Prüfungskompetenz erheblich eingeschränkt. In den USA ist die Kontrolle der Geheimhaltungsentscheidung demgegenüber zunächst nicht ausdrücklich vorgesehen. Allerdings ist nach dem CIPA das Bestehen einer Offenlegungspflicht und damit inzident die Geheimhaltungsbedürftigkeit für den konkreten Fall zu prüfen. Die Entscheidung über die Offenlegungspflicht kann damit ebenfalls innerhalb des Strafverfahrens durch das Tatgericht geklärt werden.[135] Diese Kontrolle unterliegt, anders als im deutschen Recht, keinen Beschränkungen. Der CIPA scheint daher den Bedürfnissen des Betroffenen eher Rechnung zu tragen als die Vorschriften des deutschen Strafverfahrens. Bei einer Einbeziehung der Rechtsprechungspraxis relativiert sich dieser Unterschied jedoch.

---

[135] Dass dies in einem adversatorischen Verfahren auch anders geht, zeigt die im kanadischen Recht existente Entsprechung im CEA. Dort delegiert section 38 CEA die Entscheidung an ein separates Gericht; vgl. hierzu *Roach,* in: Minister of Public Works and Government Services, S. 263.

In diesem Zusammenhang wurde unter anderem auf die richterlich geschaffene Abwägungslösung verwiesen, welche nach dem CIPA die an eine Offenlegung zu stellenden Anforderungen erhöht.[136] Nach diesem richterlichen Prüfungsmaßstab muss der Angeklagte nachweisen, dass das Beweismittel für einen fairen Strafprozess selbst unter Einbeziehung der Geheimhaltungsinteressen unerlässlich ist. Da die Überprüfung zudem unter Ausschluss der Verteidigung erfolgt, kann die Verteidigung die Geheimhaltung nur auf der Grundlage von Vermutungen rügen. Von derartigen Vorträgen wird sich das Gericht nur in offensichtlichen Fällen überzeugen lassen. Die Rechtsfortbildung der amerikanischen Gerichte führt damit faktisch zu einem der Willkürkontrolle vergleichbaren Prüfungsrahmen. Im Ergebnis ist die Geheimhaltungsentscheidung nach dem CIPA zwar theoretisch vollumfänglich überprüfbar, aufgrund der Vorgaben der Rechtsprechungspraxis ist diese umfassende Prüfungskompetenz jedoch nicht automatisch mit einer erhöhten Ausgleichsfunktion für den Angeklagten verbunden. Im Vergleich zum deutschen Modell unterscheidet sich die Kompensationswirkung des CIPA damit nur unwesentlich.

Diese Erkenntnis trifft auf die Kontrollen des FISA in ähnlicher Weise zu. Im Anwendungsbereich des FISA sind sowohl die Einwirkungsmöglichkeiten des Betroffenen als auch die Prüfungskompetenz des Strafrichters massiv eingeschränkt. Der Betroffene hat aufgrund umfassender Ausschlussmöglichkeiten regelmäßig keine Möglichkeit die Offenlegung der FISA-Vorgänge zu erreichen. Da das Gericht zudem an die Beurteilungen der Exekutive bei Erlass der FISA-Anordnung gebunden ist, kann es die Geheimhaltungsentscheidung selbst nur auf offensichtliche Fehler prüfen. Der amerikanische Richter unterliegt damit ähnlichen Vorgaben wie der deutsche Strafrichter bei der Willkürkontrolle der Sperrgründe. Hierbei ist jedoch zu beachten, dass sich die Sperrerklärung regelmäßig auf das unmittelbare Beweismittel bezieht, während die Geheimhaltungsentscheidung im FISA überwiegend die FISA-Vorgänge und nicht die FISA-Erkenntnisse betrifft.

Außer den Kontrollen durch das Strafgericht kann die Geheimhaltungsentscheidung weiteren nachträglichen oder zwischengeschalteten Kontrollen unterliegen. Im deutschen Recht kann die Sperrerklärung etwa über den Umweg des Verwaltungsverfahrens einer vollumfänglichen Rechtmäßigkeitskontrolle zugeführt werden. Hierzu muss der Angeklagte in einem ersten Schritt eine Anfechtungsklage gegen die Sperrerklärung erheben. Innerhalb dieses Verwaltungsverfahrens ist in einem zweiten Schritt ein spezielles Zwischenverfahren vor einem besonderen Fachsenat des Oberverwaltungsgerichts beziehungsweise des Bundesverwaltungsgerichts zu beantragen. Diesem Fachsenat wird unter Ausschluss der sonstigen Verfahrensbeteiligten voller Zugang zu den gesperrten Akten gewährt. Die dortigen Richter können damit ohne Einschränkungen über die Geheimhaltungsbedürftigkeit der gesperrten Akten entscheiden.

---

[136] Vgl. Teil 3, IV.B.4.b)aa).

Im amerikanischen Recht sind demgegenüber keine dem verwaltungsgerichtlichen *in camera*-Verfahren vergleichbaren Kontrollmöglichkeiten vorgesehen. Sowohl der CIPA als auch der FISA ermöglichen der Regierung eine Zwischenbeschwerde, ohne dem Betroffenen ebenfalls eine solche Befugnis zuzugestehen. Lehnt das amerikanische Strafgericht eine Offenlegung ab, hat der Angeklagte abseits des klassischen Rechtsmittelverfahrens keine Möglichkeit, gegen die Geheimhaltungsentscheidung vorzugehen. Die Einlegung von Rechtsmitteln ist im Vergleich zur deutschen Verwaltungskontrolle ein schwächeres Instrument, da durch diese nur insgesamt gegen die Verurteilung und nicht isoliert gegen die Geheimhaltung vorgegangen werden kann. Dieser Unterschied wird jedoch durch zwei Aspekte relativiert. Zum einen sind die deutschen Strafgerichte nicht verpflichtet, das Strafverfahren während der verwaltungsgerichtlichen Klärung auszusetzen.[137] Zum anderen kann im amerikanischen Recht ein sicherheitsgeprüfter Verteidiger zugelassen werden, der durch Zugriff auf die geheimhaltungsbedürftigen Informationen die Geheimhaltungsentscheidung rügen kann.

cc) Zwischenergebnis

Bei der vergleichenden Beurteilung der im deutschen und amerikanischen Recht bestehenden Kontrollmechanismen ergeben sich zahlreiche Unterschiede. Im Vergleich zum FISA sind im deutschen Modell die Rechtsschutzmöglichkeiten gegen eine Geheimhaltungsentscheidung stärker ausgebaut. Dieser Rechtsschutz wird zwar nicht unmittelbar innerhalb des Strafverfahrens, jedoch zumindest nachträglich beziehungsweise im Zwischenverfahren über die verwaltungsgerichtliche *in camera*-Kontrolle gewährleistet. Beim Vergleich mit dem CIPA kann demgegenüber kein eindeutiges Urteil gefällt werden. Bei einer Gesamtbetrachtung ist nur schwer beurteilbar, ob das deutsche Modell oder die strafverfahrensinternen CIPA-Kontrollen vorteilhafter sind. Der deutsche Umweg über das Verwaltungsverfahren ist sicherlich mit einem größeren Zeitaufwand verbunden als das amerikanische Modell. Allerdings werden auch im amerikanischen Recht erhebliche zeitliche Verzögerungen in Kauf genommen – so etwa wenn der Verteidiger infolge einer Schutzanordnung eine Sicherheitsüberprüfung durchlaufen muss. Umgekehrt hat die deutsche Lösung den Vorzug, dass die Kontrolle der Geheimhaltungsbedürftigkeit einem speziellen, mit Staatsschutzfragen befassten Fachsenat obliegt. Ein solches Gremium kann die staatlichen Schutzinteressen aufgrund seines Erfahrungsschatzes und Fachwissens potentiell besser beurteilen als der klassische Einzelrichter in der *discovery*.

Im Ergebnis liegen den jeweiligen Kontrollmechanismen unterschiedliche Konzepte zugrunde. Im amerikanischen Recht ist die Kontrolle der geheimdienstlichen Überwachungsmaßnahmen in die Strafgerichtsbarkeit integriert. Übertragen auf das

---

[137] Vgl. BGH NStZ 1985, S. 466f; kritisch hierzu *Fezer,* JuS 1987, S. 362.

deutsche Recht würde sich innerhalb der mit Staatsschutzstraftaten befassten Strafgerichte ebenfalls die Schaffung eines speziellen Kontrollgremiums anbieten.[138] Dieses Sondergremium könnte auf Antrag der Verfahrensbeteiligten in einem separaten Zwischenverfahren die Rechtmäßigkeit der Überwachungsmaßnahmen und das Bestehen von Offenlegungspflichten unter Beachtung von Geheimschutzregeln kontrollieren.[139] Diese Lösung hätte zwei Vorteile. Zum einen könnte sichergestellt werden, dass die Beweissurrogate nicht fälschlicherweise auf rechtswidrig erhobene Erkenntnisse gestützt werden. Zum anderen würde sich die Rechtmäßigkeit der Sperrung zeitnah und bereits vor Rechtskraft des Strafurteils entscheiden, was sich sowohl zugunsten des Angeklagten als auch positiv auf die Verfahrensökonomie auswirken würde. Umgekehrt ist jedoch zu bedenken, dass es sich bei einer Sperrerklärung um einen Verwaltungsakt handelt, welcher grundsätzlich der Kontrolle der Verwaltungsgerichte obliegt. Diese Zuständigkeitsverteilung steht einer Integration der Kontrollentscheidung in das Strafverfahren daher grundsätzlich entgegen.

b) Kompensation durch Beweissurrogation

In beiden Rechtsordnungen wird die Beweissurrogation zum Schutz geheimhaltungsbedürftiger Informationen akzeptiert.[140] Die nationalen Surrogationsmodelle unterscheiden sich vor allem danach, wie und wann die Ersetzbarkeit der Beweismittel geprüft wird.

aa) Zuständigkeit für die Beweissurrogation

Sowohl im deutschen als auch im amerikanischen Recht wird die Surrogationsentscheidung auf den Richter übertragen. Diese Aufgabenverteilung resultiert aus der jeweiligen Gestaltung der nationalen Verfahrensmodelle. Im deutschen Recht ist die Beweissurrogation insofern logische Konsequenz der richterlichen Aufklärungspflicht. Nach dieser liegt die Verantwortung für die Beweisaufnahme vor allem beim Gericht.[141] Ist das originäre Beweismittel aufgrund einer Sperrerklärung nicht erreichbar, ist der Richter zu einer Beweisführung mit mittelbaren Beweismitteln verpflichtet. Im Gegensatz dazu obliegt die Beweiserhebung in den USA grundsätzlich den Parteien, welche ihre Beweise im Wechselspiel vortragen. Bei einer Heranziehung von *classified information* begrenzt der CIPA die Beweisfüh-

---

[138] Zur Ansiedelung eines speziellen Zwischenverfahrens innerhalb der Strafgerichtsbarkeit vgl. SK-StPO-*Wohlers,* § 96 Rn. 35.

[139] Vgl. zu dieser Idee unabhängig vom amerikanischen Kontext *Graulich,* in: Graulich/Simon, S. 160ff, unter Verweis auf die Vorbilder in §§ 99, 189 VwGO. Ähnlich *Gaede,* StV 2006, S. 605ff.

[140] Der Vergleich beschränkt sich auf den CIPA, da im Rahmen des FISA die unmittelbaren Erkenntnisse offen gelegt werden und keine Beweissurrogation notwendig ist.

[141] Vgl. zur unterschiedlichen Richterrolle *King,* Int'l Legal Persp. (12) 2002, S. 207f.

rungsmöglichkeiten aus Geheimschutzgründen allerdings auf die Informationen, die für eine faire Verfahrensgestaltung notwendig sind. Zu diesem Zweck filtert der Richter unter anderem die den Geschworenen vorlegbaren Beweissurrogate. Die durch die Ersetzbarkeitsprüfung erfolgende Beschränkung der Beweisführungsrechte ist insofern mit der des deutschen Beweisantragsrechts bei einer sperrbedingten Unerreichbarkeit vergleichbar.

bb) Zeitpunkt der Beweissurrogation

Von diesen Gemeinsamkeiten abgesehen erfolgt die Surrogationsentscheidung in beiden Rechtsordnungen zu unterschiedlichen Zeitpunkten. Im amerikanischen Recht wird die Surrogationsfrage bereits im Vorfeld der Hauptverhandlung geklärt, um die Geschworenen vor einer unsachgemäßen Beeinflussung zu schützen. In der Konsequenz muss die Verteidigung ihre Strategie vorab und vorausschauend planen.[142] Demgegenüber werden im deutschen Vorverfahren zwar ebenfalls wesentliche Weichen gestellt, die Unerreichbarkeit selbst wird jedoch erst in der Hauptverhandlung geprüft.[143] Anders als im amerikanischen Kontext kann der deutsche Richter etwa infolge eines Beweisantrages oder aufgrund der allgemeinen Aufklärungspflicht jederzeit in die Beweisaufnahme eintreten und die Un-/Erreichbarkeit eines Beweismittels prüfen.[144] Während die Exekutive im amerikanischen Recht bereits im Vorfeld erfährt, wie das Gericht mit den Beweismitteln umzugehen beabsichtigt, sind die Konsequenzen der Beweissurrogation im deutschen Recht weit weniger vorhersehbar. Dort erlaubt lediglich die gerichtliche Gegenvorstellung eine Einschätzung des mit der Geheimhaltung verbundenen Risikos. Da die Regierung bei einer nachteiligen Gegenvorstellung die Sperrgründe jedoch nachbessern kann, sind die Risiken für die Exekutive vergleichbar gering.

cc) Entscheidungsgrundlage für die Beweissurrogation

Weitere Unterschiede ergeben sich in Bezug auf die Entscheidungsgrundlage, die der Beweissurrogation zugrunde liegt. Anders als im CIPA-Verfahren trifft der deutsche Richter seine Entscheidung ohne unmittelbare Kenntnisnahme des gesperrten Beweismittels. Dieser Unterschied beruht auf den jeweils unterschiedlichen Richterfunktionen. Im deutschen Recht ist der Richter für die Urteilsfindung zuständig. Ihm dürfen deshalb keine Informationen zugänglich gemacht werden, die dem Angeklagten gegenüber geheim bleiben. Da mit einer Sperrerklärung gerade kein Beweisverbot verbunden ist, wäre der Richter bei einer Zugriffsmöglichkeit nach dem Amtsermittlungsgrundsatz umgekehrt sogar zur Einführung des Be-

---

142 So *Perron,* Beweisantragsrecht, S. 435.

143 Vgl. KK-*Fischer,* § 244 Rn. 156.

144 Vgl. KK-*Schoreit,* § 258 Rn. 2.

weismittels verpflichtet.[145] Im Gegensatz dazu ist der amerikanische Richter nicht unmittelbar am endgültigen Schuldspruch beteiligt. Er prüft lediglich, welche Beweissurrogate den Geschworenen vorgelegt werden dürfen. Die Aufgabenteilung zwischen Richter und Geschworenen stellt in diesem Zusammenhang letztlich sicher, dass die Beweissurrogation nicht mit Blick auf den Verfahrensausgang entschieden wird.[146] In beiden Rechtsordnungen wird damit zwischen den Instanzen unterschieden, die für die Überprüfung der Geheimhaltung einerseits und die Urteilsfindung andererseits zuständig sind. Sowohl im deutschen als auch im amerikanischen Recht darf der für den Schuldspruch zuständige Entscheidungsträger nur auf diejenigen Beweismittel Zugriff haben, die auch der Verteidigung zugänglich sind. Aufgrund der Zweiteilung im amerikanischen Recht werden daher tendenziell weniger Beweissurrogate zugelassen als im deutschen Strafverfahren. Während im CIPA insofern eine Surrogation bei einer drohenden Irreführung der Geschworenen ausscheidet, wird im deutschen Kontext ein Beweisantrag erst bei offensichtlicher Ungeeignetheit des Beweismittels abgelehnt. Eine Eingrenzung erfolgt dort erst auf der Ebene der Beweiswürdigung.

dd) Arten möglicher Beweissurrogate

Schließlich ist der Umfang der rechtlich vorgesehenen Beweissurrogate in beiden Rechtsordnungen sehr unterschiedlich. Bei einer Nutzung von *classified information* sind im CIPA ausdrücklich nur drei taugliche Beweissurrogate vorgesehen, während das deutsche Surrogationsrecht sehr viel mehr Ersetzungsmöglichkeiten zur Verfügung stellt. Im amerikanischen Recht stehen insofern lediglich die Löschung der geheimhaltungsbedürftigen Passagen, die Substitution durch zusammenfassende Darstellungen oder eine Wahrunterstellung zur Auswahl. Demgegenüber kommen in Deutschland die Nutzung von Urkunden, die Verlesung von Niederschriften einer polizeilichen Vernehmung oder aber die Vernehmung eines Zeugen vom Hörensagen in Betracht.

Dieser Unterschied kann zum Teil erneut auf die Beteiligung der Geschworenen an der Entscheidungsfindung zurückgeführt werden. Zwar können die Geschworenen den Beweiswert eines vorgelegten Beweismittels ebenfalls herabstufen, für ein Laiengremium ist dies jedoch wesentlich schwieriger als für einen juristisch ausgebildeten Richter. Im Grundsatz sollen den Geschworenen daher nur verlässliche und glaubwürdige Beweismittel beziehungsweise Surrogate vorgelegt werden. Im deutschen Recht obliegt die Beweiswürdigung demgegenüber dem Richter, dem aufgrund seiner Fachkompetenz die angemessene Würdigung zweifelhafter Beweise zugetraut wird. Einen weiteren Erklärungsansatz liefert die im deutschen Recht

---

[145] In BGH StV 1993, S. 170f wird dementsprechend ein Beweisverbot trotz rechtmäßiger Sperrung verneint.

[146] So *Perron,* Beweisantragsrecht, S. 398.

maßgebliche Orientierung am materiellen Wahrheitsbegriff.[147] Danach gebietet die richterliche Aufklärungspflicht eine erschöpfende Sachverhaltsaufklärung und damit beim Fehlen unmittelbarer Erkenntnisse zumindest die ersatzweise Heranziehung von Beweissurrogaten.[148] Demgegenüber soll nach dem formalisierten Wahrheitsverständnis des amerikanischen Rechts die Wahrheit nicht durch eine historische Rekonstruktion des Tatgeschehens, sondern durch den Wettstreit im Haupt- und Kreuzverhör und damit durch die Gewährleistung der Verfahrensgerechtigkeit hergestellt werden.[149] Da die Einführung von Beweissurrogaten die adversatorische Beweispräsentation einschränkt, ist sie theoretisch auf wenige Ausnahmen zu limitieren. Eine Beweissurrogation nach dem CIPA wird daher nur in den gesetzlich vorgesehenen Fällen und nur bei einer Gewährleistung vergleichbarer Verteidigungsmöglichkeiten zugelassen. Diese strikten Vorgaben wirken sich in der praktischen Anwendung allerdings kaum aus. Es ist kein Fall bekannt, in dem die Richter eine Ersetzung nach dem CIPA abgelehnt haben.[150] Durch diese Tendenz wird die Surrogation von *classified information* zum Regelfall, wodurch sich das formalisierte Gerechtigkeitsverständnis des amerikanischen Rechts zumindest im Bereich der schweren Kriminalität zunehmend einem materiellen Wahrheitsbegriff annähert.[151]

c) Kompensation durch sonstige Mechanismen

Die beschriebenen Kompensationsmöglichkeiten werden in beiden Rechtsordnungen durch weitere Mechanismen ergänzt. Im deutschen Recht ist dies vor allem das Institut der vorsichtigen beziehungsweise hypothetischen Beweiswürdigung, während im amerikanischen Recht anderweitige Sanktionen im Vordergrund stehen. Zwar finden sich die einzelnen Konzepte in ähnlicher Form jeweils auch in der anderen Rechtsordnung, bei der Lösung der Geheimhaltungsproblematik kommt ihnen jedoch zum Teil ein sehr unterschiedliches Gewicht zu.

In den Landesberichten konnten für beide Verfahrensordnungen Elemente der Beweiswürdigung nachgewiesen werden. Im deutschen Strafverfahren wird die Beweiswürdigung nach § 261 StPO durch den Richter vorgenommen, während diese Aufgabe in den USA den Geschworenen obliegt.[152] Grundlage der Überzeugungsbildung sind jeweils die Erkenntnisse, die Gegenstand der Hauptverhandlung waren. Die zuständigen Instanzen haben zu diesem Zweck die gleiche Tatsachenkenntnis wie der Angeklagte. Der an den Schuldspruch zu stellende Grad an Über-

---

147 Vertiefend bei *Roxin/Schünemann,* § 15 Rn. 3ff.

148 Vgl. *Perron,* Beweisantragsrecht, S. 462.

149 So *Trüg,* S. 66

150 Vgl. hierzu stellvertretend *Turner/Schulhofer,* S. 29.

151 Zu dieser allgemeinen Tendenz vgl. *Trüg,* S. 358f, 382f.

152 Vgl. allgemein *Perron,* Beweisantragsrecht, S. 458.

zeugung ist ebenfalls vergleichbar.[153] In beiden Rechtsordnungen ist für eine Verurteilung insofern ein ausreichendes Maß an Sicherheit notwendig.[154] Dem amerikanischen Beweisstandard des *proof beyond a reasonable doubt* steht im deutschen Recht allgemein ein zweigeteilter Standard aus freier Beweiswürdigung und Zweifelssatz gegenüber.

Dem Konzept der Beweiswürdigung wird bei der Lösung der Geheimhaltungsproblematik allerdings ein jeweils unterschiedlicher Stellenwert beigemessen. Im deutschen Geheimhaltungsmodell wird die Beweiswürdigung als primärer Kompensationsmechanismus angesehen.[155] Die mit der Geheimhaltung verbundenen Defizite sollen durch eine Herabstufung des Beweiswerts sowie durch eine vorsichtige Beweiswürdigung unter Heranziehung des Zweifelssatzes kompensiert werden. Die flexible Beweiserhebung unter Rückgriff auf mittelbare Beweismittel wird im deutschen Modell damit auf Ebene der Beweiswürdigung komplementiert.

In den USA ist die Geheimhaltung demgegenüber sehr viel früher zu kompensieren. Zur Gewährleistung vergleichbarer Verteidigungsmöglichkeiten kann der Richter auf der Grundlage des CIPA etwa die Zurverfügungstellung bestimmter Erkenntnisse oder Beweissurrogate verlangen. Bei der Missachtung einer entsprechenden Anordnung sieht der CIPA als mögliche Sanktion unter anderem eine vollständige oder teilweise Verfahrenseinstellung vor. Im deutschen Recht ist eine solche Konsequenz demgegenüber nur in außergewöhnlichen Fällen erforderlich, etwa wenn der Richter infolge der Geheimhaltung keine verantwortbare Überzeugung mehr bilden kann oder dem Verfahren insgesamt die Grundlage entzogen wurde.[156] Ein Prozesshindernis wird im deutschen Strafverfahren folglich nur in seltenen Ausnahmefällen angenommen, während in den USA die Verfahrenseinstellung eine der zentralen Sanktionen darstellt. Die in der deutschen Wissenschaft zum Teil bestehenden Forderungen nach einer Sanktionierung der staatlich verkürzten Beweisgrundlage durch die Annahme eines Beweisverbots oder einer Wahrunterstellung haben sich in der Praxis bislang nicht durchgesetzt.

Im Vergleich zum amerikanischen Ansatz bleibt die im deutschen Recht favorisierte Beweiswürdigungslösung in ihrer kompensatorischen Wirkung hinter der Möglichkeit einer Verfahrenseinstellung zurück. Bei der Beweiswürdigungslösung

---

153 So im Ergebnis *Feeney/Herrmann,* S. 401f, 430.

154 Vgl. California Criminal Jury Instr., CalCrim No. 220: "leaves you with an abiding conviction that the charge is true. The evidence need not eliminate all possible doubt because everything in life is open to some possible or imaginary doubt. In deciding […] you must impartially compare and consider all the evidence that was received throughout the entire trial". Im Vergleich fordert BGH NJW 1951, S. 122, „ein nach der Lebenserfahrung ausreichendes Maß an Sicherheit […], dem gegenüber vernünftige Zweifel nicht mehr laut werden können." Die bloße „theoretische" oder „abstrakte" Möglichkeit, dass der Angeklagte nicht der Täter war, kann seine Verurteilung nicht hindern.

155 Zum deutschen Modell vgl. *Gusy,* Grundrechte, S. 115; *Kornblum,* S. 324.

156 Vgl. bereits Teil 4, V.A. sowie BGH NStZ 2004, S. 343f.

handelt es sich um ein generelles Abwägungsmodell, das dem Richter zum Teil erhebliche Fähigkeiten abverlangt. Vor allem in Bezug auf das Institut der hypothetischen Beweiswürdigung wird zum Teil die praktische Umsetzbarkeit bezweifelt. Im CIPA wird der Angeklagte demgegenüber nicht auf einen pauschalen Nachteilsausgleich verwiesen, sondern kann gegebenenfalls von einer Verfahrenseinstellung profitieren. Allerdings kann auch im amerikanischen Recht von dieser Sanktion abgesehen werden, wenn die Regierung darlegen kann, dass eine Verfahrenseinstellung dem Gerechtigkeitsempfinden widersprechen würde. In diesem Fall ist das deutsche Strafgericht besser in der Lage, die mit der Beweissurrogation verbundenen Nachteile auszugleichen, als das mit Laien besetzte Geschworenengremium. In diesem Zusammenhang hat die Beweiswürdigungslösung den Vorteil, dass die Beeinträchtigungen einer Geheimhaltungsentscheidung bis zum Abschluss des Strafverfahrens berücksichtigt werden können.

Teil 5

Schlussbetrachtung

Die Nutzung von Geheimdienstinformationen im Strafprozess wirft zwei komplexe Fragestellungen auf. Zum einen geht es um die Frage, inwieweit Informationen der Nachrichtendienste generell im Strafprozess als Beweismittel herangezogen werden dürfen und inwiefern etwaige Besonderheiten Berücksichtigung finden. Zum anderen geht es um den Schutz sicherheitsrelevanter Informationen vor einer vollständigen Offenlegung im Strafverfahren und dem Ausgleich dieser Geheimhaltungsinteressen mit den Belangen einer effektiven Strafverteidigung. Diesen beiden Themenkomplexen liegen im deutschen und amerikanischen Recht im Ausgangspunkt völlig entgegengesetzte Lösungsmodelle zugrunde. Während in Deutschland die Sicherheitsbehörden durch das Trennungsgebot und die Unterscheidung in Prävention und Repression rechtlich und institutionell deutlich voneinander getrennt sind, fehlt in den USA eine solche Aufteilung fast vollständig. Das FBI etwa vereint vielmehr polizeiliche und geheimdienstliche Komponenten in einer einzigen Behörde. Eine Unterscheidung zwischen repressiven und präventiven Aufgaben ist dem amerikanischen Recht ebenfalls fremd. Dieser Aspekt erweist sich aus der deutschen Perspektive als besonders fundamental, da die Differenzierung zwischen Prävention und Repression bis heute der Dreiteilung zwischen Geheimdiensten, Polizei und Strafverfolgungsbehörden zugrunde liegt. Die Weitergabe von Informationen der Nachrichtendienste an das Justizsystem ist in den USA damit sehr viel unproblematischer als im deutschen Kontext, da beide Ermittlungsstränge entweder aufgrund einer institutionellen Verschmelzung bereits über einen identischen Wissensstand verfügen oder aber ähnlichen Erhebungsvoraussetzungen unterliegen.

Zusätzlich zu den Unterschieden in der Sicherheitsarchitektur entstammen das deutsche und amerikanische Strafverfahren unterschiedlichen Rechtskreisen. Während der deutsche Strafprozess inquisitorischen Grundstrukturen folgt, wird der amerikanische Strafprozess durch adversatorische Elemente geprägt. Ausgehend von diesen unterschiedlichen Verfahrensstrukturen werden die nationalen Offenlegungs- und Geheimhaltungsregeln durch sehr unterschiedliche Gesichtspunkte bestimmt. Während die strafprozessualen Konsequenzen einer Sperrerklärung in Deutschland vor allem der richterlichen Verantwortung überlassen werden, finden sich in den USA mit dem CIPA und FISA ausdifferenzierte Vorschriften, die eine Offenlegung gegenüber den Geschworenen verhindern. Aufgrund dieser andersartigen Strukturierung des Geheimdienstsektors einerseits und der abweichenden Strafverfahrensmodelle andererseits bietet der Vergleich des deutschen

und amerikanischen Rechts eine Vielzahl von Herausforderungen und Kontrastmöglichkeiten.

Bei der rechtsvergleichenden Bearbeitung der Fragestellung auf der Grundlage einer funktionalen Betrachtung wurden für beide Problemkreise wichtige Erkenntnisse erzielt. Im deutschen und amerikanischen Recht konnte der Einfluss der Sicherheitsarchitektur auf die Nutzung von Geheimdienstinformationen nachgewiesen werden. Die Anforderungen des Trennungsgebots, des Sicherheitsföderalismus sowie die Vorgaben des ersten und vierten Verfassungszusatzes prägen die Konzeption der Nachrichtendienste, die Zusammenarbeit mit dem Strafverfolgungssektor und die konkrete Verwertbarkeit als Beweismittel. Aufgrund der weitgehenden Verschmelzung der amerikanischen Sicherheitsbehörden steht das amerikanische Recht einer Übermittlung und Verwertung von Geheimdienstinformationen grundsätzlich offen gegenüber. Demgegenüber wird im deutschen Recht die Nutzung von Geheimdienstinformationen vor allem durch die Vorgaben des Trennungsgebots begrenzt. Eine strafprozessuale Nutzung ist in Deutschland bislang nur bei schweren beziehungsweise staatsschutzrelevanten Straftaten vorgesehen. Die dem deutschen Recht bekannte und historisch verwurzelte Aufteilung in nachrichtendienstliche, polizeiliche und strafrechtliche Ermittlungsfelder verliert jedoch zunehmend an Trennschärfe. Vor allem in jüngster Zeit wurden die bislang streng regulierten Überwachungs- und Übermittlungsbefugnisse der einzelnen Sicherheitsbehörden unter Verweis auf Bedrohungen der nationalen Sicherheit ausgeweitet und damit ein Wandel der nationalen Sicherheitsarchitektur angestoßen.

Die staatlicherseits bestehenden Sicherheitsbedürfnisse werden im Rahmen des zweiten Themenkreises, der sogenannten Geheimhaltungsproblematik, ebenfalls deutlich. Bei einer Nutzung von Geheimdienstinformationen stehen sowohl der deutsche als auch der amerikanische Staat vor dem Dilemma, wie gleichzeitig den Offenlegungspflichten des Strafverfahrens einerseits und den Geheimhaltungsinteressen der Nachrichtendienste andererseits gerecht zu werden ist. Die Zusammenarbeit der Geheimdienste mit den Strafverfolgungsbehörden führt in beiden Rechtsordnungen zu erheblichen Rechts- und Interessenskonflikten. In Deutschland wird dieses in Geheimhaltungsfragen bestehende Spannungsverhältnis vor allem durch die Heranziehung von Beweissurrogaten gelöst. Die staatlich verkürzte Beweisgrundlage wird durch eine vorsichtige Beweiswürdigung, die Minderung im Beweiswert und den Zweifelssatz berücksichtigt. Bei einer Zurückhaltung entlastenden Beweismaterials wird diese Lösung zusätzlich durch das Konstrukt der hypothetischen Beweiswürdigung ergänzt. Im amerikanischen Strafverfahren werden demgegenüber die wesentlichen Entscheidungen bereits im Vorfeld der Hauptverhandlung getroffen. Diese vorgeschaltete richterliche Kontrolle dient dazu, die Offenlegung irrelevanter, aber schutzwürdiger Informationen zu verhindern und eine sichere Nutzung notwendiger Erkenntnisse zu gewährleisten. Lediglich die richterlich vorsortierten Beweissurrogate werden den Geschworenen als Beweismittel vorgelegt. Da die Geschworenen vor irreführenden Informationen geschützt wer-

den müssen, sind die zulässigen Beweissurrogate gesetzlich begrenzt. Solche Schutzvorkehrungen sind aufgrund der Fachkompetenz des deutschen Strafrichters nicht erforderlich. Die zugelassenen Beweissurrogate können von diesem im Wege der vorsichtigen Beweiswürdigung in ihrem Beweiswert herabgestuft werden.

Die Nutzung von Geheimdienstinformationen im Strafverfahren wird bei einer abschließenden Betrachtung in beiden Rechtsordnungen maßgeblich durch die Person des Strafrichters beeinflusst. Dieser soll als Garant sowohl eine effektive Strafverfolgung als auch ein faires Strafverfahren gewährleisten. Entsprechend den Besonderheiten der Sicherheitsarchitektur und der Strafverfahrensregeln greifen die jeweiligen Schutzmechanismen jedoch zu unterschiedlichen Zeitpunkten und in unterschiedlicher Intensität. Im deutschen Recht nimmt der Strafrichter seine Verantwortung vor allem im zeitlichen Umfeld der Hauptverhandlung wahr. In dieser muss er den geheimdienstlichen Ursprung über das Institut des hypothetischen Ersatzeingriffs berücksichtigen und eine Nichtoffenlegung über Beweissurrogate sowie eine vorsichtige Beweiswürdigung ausgleichen. Im amerikanischen Recht soll ebenfalls der Strafrichter eine Umgehung strafprozessualer Garantien verhindern. Diese Aufgabe wird über die Vorgaben des vierten Verfassungszusatzes zum Teil bereits im Rahmen der Informationserhebung berücksichtigt, indem etwa ein klassischer *warrant* oder ein FISA-*warrant* vorliegen muss. In Geheimhaltungsfragen greifen wiederum die Surrogationsmechanismen des FISA und des CIPA, mittels derer der Strafrichter vorab die geheimdienstlichen Erkenntnisse auf das für einen fairen Prozess erforderliche Maß reduziert. Trotz der im Ausgangspunkt sehr unterschiedlichen Grundmodelle werden bei einer funktionalen Betrachtung damit zugleich wesentliche Gemeinsamkeiten beider Rechtsordnungen deutlich.

Literaturverzeichnis

Adam, Jürgen, Aktuelle Rechtsprechung des BVerfG zum Strafrecht und Strafprozessrecht. NStZ 2010, S. 321–325.

Albers, Marion, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge. Schriften zum Öffentlichen Recht, Bd. 842. Berlin 2001.

Albert, Helmut, Das „Trennungsgebot" – ein für Polizei und Verfassungsschutz überholtes Entwicklungskonzept? ZRP 1995, S. 105–109.

– Informationsverarbeitung durch Nachrichtendienste am Beispiel der Verfassungsschutzbehörden. In: Guido Korte/Manfred Zoller (Hrsg.), Informationsgewinnung mit nachrichtendienstlichen Mitteln. Rahmenbedingungen, Einsatzmodalitäten, Verarbeitungsaspekte. Brühl/Rheinland 2001, S. 88–110 [zit.: *Albert,* in: Korte/Zoller].

Albrecht, Markus, OSINT-Management unter neuen Vorzeichen. In: Heiko Borchert (Hrsg.), Verstehen, dass die Welt sich verändert hat. Neue Risiken, neue Anforderungen und die Transformation der Nachrichtendienste. Baden–Baden 2005, S. 44–56 [zit.: *Albrecht,* in: Borchert].

Albrecht, Peter-Alexis, Vom Unheil der Reformbemühungen im Strafverfahren. Bemerkungen zum Strafverfahrensänderungsgesetz vom 1.11.2000. StV 2001, S. 416–420.

Allgayer, Peter/Klein, Oliver, Verwendung und Verwertung von Zufallserkenntnissen. wistra 2010, S. 130–133.

Amelung, Knut, Grundfragen der Verwertungsverbote bei beweissichernden Haussuchungen im Strafverfahren. NJW 1991, S. 2533–2540.

– Die Verwertbarkeit rechtswidrig gewonnener Beweismittel zugunsten des Angeklagten und deren Grenzen. StraFo 1999, S. 181–186.

Arloth, Frank, Neue Wege zur Lösung des strafprozessualen „V-Mann-Problems" – Durch Beschlagnahme von Behördenakten? NStZ 1993, S. 467–470.

Artzt, Matthias, Die verfahrensrechtliche Bedeutung polizeilicher Vorfeldermittlungen. Zugleich eine Studie zur Rechtsstellung des von Vorfeldermittlungen betroffenen Personenkreises. Frankfurt a.M. 2000.

Arzt, Clemens, Polizeiliche Überwachungsmaßnahmen in den USA. Grundrechtsbeschränkungen durch moderne Überwachungstechniken und im War on Terrorism. Frankfurt a.M. 2004.

– Präventionsstaat zwischen Rechtsgüterschutz und Abbau von Freiheitsrechten in den USA. In: Kurt Graulich/Dieter Simon (Hrsg.), Terrorismus und Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Perspektiven. Berlin 2007, S. 241–271 [zit.: *Arzt,* in: Graulich/Simon].

Asbrock, Bernd, „Zum Mythos des Richtervorbehalts“ als wirksames Kontrollinstrument im Zusammenhang mit besonderen polizeilichen Eingriffsbefugnissen. KritV 1997, S. 255–262.

Backes, Otto/Gusy, Christoph, Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung. Frankfurt a.M./New York 2003.

Backhaus, Vera, Der gesetzliche Richter im Staatsschutzstrafrecht. Zur Verfassungsmäßigkeit des § 120 Abs. 2 GVG. Frankfurt a.M. 2010.

Bader, Johann/Ronellenfitsch, Michael, Beck’scher Online-Kommentar VwVfG, Stand: 1.1.2012, 14. Edition [zit.: Bader/Ronellenfitsch-*Bearbeiter*].

Baier, Maximilian, Die parlamentarische Kontrolle der Nachrichtendienste und deren Reform. Hamburg 2009.

Baker, Stewart, Should Spies be Cops? Foreign Policy (97) Winter 1994–1995, S. 36–52.

Baldus, Manfred, Nachrichtendienste – Beobachtung völkerverständigungswidriger Bestrebungen. ZRP 2002, S. 400–404.

Baum, Gerhart/Schantz, Peter, Die Novelle des BKA-Gesetzes. Eine rechtspolitische und verfassungsrechtliche Kritik. ZRP 2008, S. 137–140.

Baumann, Fritz-Achim, Verfassungsschutz und Polizei. Trennungsgebot und Pflicht zur Zusammenarbeit. In: Franz Josef Düwell (Hrsg.), Anwalt des Rechtsstaates. Festschrift für Diether Posser zum 75. Geburtstag. Köln 1997, S. 299–308.

Baumann, Karsten, Vernetzte Terrorismusbekämpfung oder Trennungsgebot? Möglichkeiten und Grenzen der Zusammenarbeit von Polizei und Nachrichtendiensten. DVBl 2005, S. 798–805.

Bäumler, Helmut, Das neue Geheimdienstrecht des Bundes. NVwZ 1991, S. 643–645.

Bazan, Elizabeth, The Foreign Intelligence Surveillance Act: An Overview of Selected Issues. CRS 7. Juli 2008, RL34279, S. 1–21.

Becker, Steven, XVIIIth International Congress of Penal Law. RIDP/IRPL 2009, S. 341–354.

Beling, Ernst von, Grenzlinien zwischen Recht und Unrecht in der Ausübung der Strafrechtspflege. Rede des Rektors am Geburtstage des Königs 1913. Tübingen 1913.

Berman, Emily, Domestic Intelligence: New Powers, New Risks 2011 [abrufbar unter: http://brennan.3cdn.net/b80aa0bab0b425857d_jdm6b8776.pdf; Stand: 1.5.2012].

Bernsmann, Klaus/Jansen, Kirsten, Heimliche Ermittlungsmethoden und ihre Kontrolle – Ein systematischer Überblick. StV 1998, S. 217–231.

Bertram, Konstantin, Die Verwendung präventiv-polizeilicher Erkenntnisse im Strafverfahren. Rechtsfragen im Kontext bereichsübergreifender Zweckänderungen vor dem Hintergrund eines informationellen Persönlichkeitsschutzes. Baden-Baden 2009.

Best, Richard, Intelligence Information: Need-to-Know vs. Need-to-Share. CRS 6. Juni 2011, R41848, S. 1–13.

Beukelmann, Stephan, Vorratsdatenspeicherung so nicht verfassungsgemäß. NJW-Spezial 2010, S. 184.

Beulke, Werner, Strafprozessrecht. 11. Aufl. Heidelberg 2010.

Birkenstock, Gregory, The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis. Geo. L. J. (80) 1992, S. 843–871.

Bjelopera, Jerome, Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress. CRS 10. Juni 2011, R40901, S. 1–23.

Boerman, Brian, Beyond the Wire: An Analysis of Non-Telephonic Conversations under Title III. N.Y.U. J.L. & Liberty (3) 2008, S. 599–630.

Boldt, Hans/Stolleis, Michael, Geschichte der Polizei in Deutschland. In: Hans Lisken/Erhard Denninger/Frederik Rachor (Hrsg.), Handbuch des Polizeirechts. Gefahrenabwehr, Strafverfolgung, Rechtsschutz. 4., neu bearb. u. erw. Aufl. München 2007, S. 1–41 [zit.: *Boldt/Stolleis*, in: Lisken/Denninger/Rachor].

Borgs-Maciejewski, Hermann/Ebert, Frank, Das Recht der Geheimdienste. Kommentar zum Bundesverfassungsschutzgesetz (Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes) sowie zum G 10 (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Gesetz zu Artikel 10 Grundgesetz), nebst Sammlung aller einschlägigen Gesetze des Bundes und der Länder sowie einer Chronik der Nachrichtendienste. München 1986 [zit.: Borgs-Maciejewski/Ebert-*Bearbeiter*].

Bradley, Alison, Extremism in the Defense of Liberty? The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT. Tul. L. Rev. (77) 2002, S. 465–493.

Brand, Oliver, Grundfragen der Rechtsvergleichung. Ein Leitfaden für die Wahlfachprüfung. JuS 2003, S. 1082–1091.

Brissa, Enrico, Militärischer Auslandsgeheimdienst der Bundeswehr? Grundlagen und Grenzen des „Militärischen Nachrichtenwesens. DöV 2011, S. 391–398.

Brodersen, Kilian, Das Strafverfahrensänderungsgesetz 1999. NJW 2000, S. 2536–2542.

Brüning, Janique, Die Rechtsfolgen eines Verstoßes gegen den Richtervorbehalt. Zugleich eine Anmerkung zum Urteil des BGH vom 18. April 2007. HRRS 2007, S. 250–255.

Bull, Hans, Sind Nachrichtendienste unkontrollierbar? Zu der Diskussion über die parlamentarische Kontrolle des Einsatzes nachrichtendienstlicher Mittel am Beispiel Sachsen. DöV 2008, S. 751–759.

– Informationelle Selbstbestimmung – Vision oder Illusion? Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit. Tübingen 2009 [zit.: *Bull,* Datenschutz].

Bundesamt für Verfassungsschutz, Verfassungsschutz – Was wir für sie tun [abrufbar unter: www.verfassungsschutz.de/download/SHOW/broschuere_0803_was_wir_tun.pdf; Stand: 1.5.2012; zit.: Bundesamt für Verfassungsschutz].

Bung, Jochen, Verhandlung über die Entlassung des Zeugen und Augenscheinseinnahme in Abwesenheit des gemäß § 247 StPO entfernten Angeklagten als Fälle des absoluten Revisionsgrundes nach § 338 Nr. 5 StPO. HRRS 2010, S. 50–54.

Burch, James, A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Secu-

rity. Homeland Security Affairs 3, Ausgabe 2. Juni 2007 [abrufbar unter: www.hsaj.org/?article=3.2.2; Stand: 1.5.2012].

Burhoff, Detlef, Handbuch für das strafrechtliche Ermittlungsverfahren. 4. Aufl. Münster 2006.

Carter, David, Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies [abrufbar unter: www.cops.usdoj.gov/pdf/e09042536.pdf; Stand: 1.5.2012].

Chesney, Robert, Terrorism and Criminal Prosecutions in the United States. In: Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Canada), Research papers, Vol. 3. Ottawa 2010, S. 81–148 [zit.: *Chesney,* in: Commission of Inquiry].

Chiarella, Louis/Newton, Michael, "So Judge, How Do I Get That FISA Warrant?": The Policy and Procedure for Conducting Electronic Surveillance. Army Law. Oktober 1997, S. 25–36.

Cole, David, Imaginary Walls and Unnecessary Fixes 2005 [abrufbar unter: http://apps.americanbar.org/natsecurity/patriotdebates/218-2#rebuttal; Stand: 1.5.2012].

Cowan, Cameron, Domestic Intelligence. A New Framework for the U.S. 2011 [abrufbar unter: http://independent.academia.edu/CameronCowan/Papers/753778/Domestic_Intelligence; Stand: 1.5.2012].

Daun, Anna, Die deutschen Nachrichtendienste. In: Thomas Jäger/Anna Daun (Hrsg.), Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009, S. 56–77 [zit.: *Daun,* in: Jäger/Daun].

– Auge um Auge? Intelligence-Kooperation in den deutsch-amerikanischen Beziehungen (Globale Gesellschaft und internationale Beziehungen). Wiesbaden 2011 [zit.: *Daun,* Auge um Auge].

– Nachrichtendienste in der deutschen Außenpolitik. In: Thomas Jäger/Alexander Höse/Kai Oppermann (Hrsg.), Deutsche Außenpolitik, Sicherheit, Wohlfahrt, Institutionen und Normen. Wiesbaden 2011, S. 171–197 [zit.: *Daun,* in: Jäger/Höse/Oppermann].

Dencker, Friedrich, Verwertungsverbote und Verwendungsverbote im Strafprozeß. In: Albin Eser/Jürgen Goydke/Kurt Rüdiger Maatz/Dieter Meurer (Hrsg.), Strafverfahrensrecht in Theorie und Praxis. Festschrift für Lutz Meyer-Goßner zum 65. Geburtstag. München 2001, S. 237–255.

Denninger, Erhard, Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf informationelle Selbstbestimmung. ZRP 1981, S. 231–235.

– Verfassungsschutz, Polizei und die Bekämpfung der Organisierten Kriminalität. KritV 1994, S. 232–241.

– Polizeiaufgaben. In: Hans Lisken/Erhard Denninger/Frederik Rachor (Hrsg.), Handbuch des Polizeirechts. Gefahrenabwehr, Strafverfolgung, Rechtsschutz. 4., neu bearb. u. erw. Aufl. München 2007, S. 299–397 [zit.: *Denninger,* in: Lisken/Denninger/Rachor].

Detter, Klaus, Der Zeuge vom Hörensagen – eine Bestandsaufnahme. NStZ 2003, S. 1–9.

– Einige Gedanken zu audiovisueller Vernehmung, V-Mann in der Hauptverhandlung und der Entscheidung des Bundesgerichtshofs in der Sache EI Motassadeq. StV 2006, S. 544–551.

Diemer, Herbert, Erhebungen des Generalbundesanwalts zur Klärung des Anfangsverdachts im Rahmen von ARP-Vorgängen. NStZ 2005, S. 666–669.

Donohue, Laura K., The Shadow of State Secrets. U. Pa. L. Rev. (159) 2010, S. 77–216.

Doyle, Charles, Reasonable Suspicion, and Reasonableness Standards in the Context of the Fourth Amendment and the Foreign Intelligence Surveillance Act. CRS 30. Januar 2006, S. 1–8.

– National Security Letters: Proposals in the 112th Congress. CRS 30. Juni 2011, R41619, S. 1–29.

– Terrorism, Miranda, and Related Matters. CRS 24. April 2013, R41252, S. 1–10.

Droste, Bernadette, Nachrichtendienste und Sicherheitsbehörden im Kampf gegen organisierte Kriminalität. Versuch einer Bestandsaufnahme mit Blick auf das Ausland. Köln 2002 [zit.: *Droste*, Nachrichtendienste].

– Handbuch des Verfassungsschutzrechts. Stuttgart u.a. 2007 [zit.: *Droste*, Handbuch].

Eisenberg, Ulrich, Beweisrecht der StPO. 7. Aufl. München 2011.

– Grundsätzliche erstinstanzliche Nichtzuständigkeit von Bundesanwaltschaft und Oberlandesgerichten in Jugendstrafverfahren (§ 120 GVG, § 102 JGG). NStZ 1996, S. 263–267.

Eisenberg, Ulrich/Conen, Stefan, § 152 II StPO: Legalitätsprinzip im gerichtsfreien Raum? NJW 1998, S. 2241–2249.

Eligon, John, Terror Trials in State Court: Pluses and Minuses 2011 [abrufbar unter: http://cityroom.blogs.nytimes.com/2011/05/13/terror-trials-in-state-court-pluses-and-minuses/?pagemode=print; Stand: 1.5.2012].

Elsea, Jennifer, The Protection of Classified Information: The Legal Framework. CRS 10. Januar 2011, RS21900, S. 1–12.

Engelhart, Marc, The Secret Service's Influence on Criminal Proceedings. In: Marianne Wade/Almir Maljević (Hrsg.), A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications. New York 2010, S. 505–547 [zit.: *Engelhart,* in: Wade/Maljević].

Epping, Volker/Hillgruber, Christian, Grundgesetz. 6. Aufl. München 2010 [zit.: Epping/Hillgruber-*Bearbeiter*].

Ernst, Marcus, Verarbeitung und Zweckbindung von Informationen im Strafprozeß. Berlin 1993.

Eser, Albin, Vorzugswürdigkeit des adversatorischen Prozesssystems in der internationalen Strafjustiz? Reflektionen eines Richters. In: Heinz Müller-Dietz (Hrsg.), Festschrift für Heike Jung. Zum 65. Geburtstag am 23. April 2007. Baden-Baden 2007, S. 167–187 [zit.: *Eser,* in: Müller-Dietz].

Evans, Jennifer, Hijacking Civil Liberties: The USA PATRIOT Act of 2001. Loy. U. Chi. L.J. (33) 2002, S. 933–990.

Farnsworth, E. Allan/Sheppard, Steve, An Introduction to the Legal System of the United States. 4. Aufl. Oxford/New York 2010.

Feeney, Floyd/Herrmann, Joachim, One Case – Two Systems. A Comparative View of American and German Criminal Justice Systems. Ardsley, New York, 2005.

Fenske, Dan, All Enemies, Foreign and Domestic: Erasing the Distinction Between Foreign and Domestic Intelligence Gathering under the Fourth Amendment. NULR (102) 2008, S. 343–382.

Ferse, Hartmut, OK – (K)eine Aufgabe für den Verfassungsschutz. KritV 1994, S. 256–261.

Fezer, Gerhard, Anfechtung einer Sperrerklärung des Innenministers und Aussetzung der Hauptverhandlung. BGH NStZ 1985, 466. JuS 1987, S. 358–363.

Forkert-Hosser, Sandra, Vorermittlungen im Strafprozessrecht. Erhebung und Verwendung von Daten vor dem Anfangsverdacht. Frankfurt u.a. 2010.

Forster, Gerhard, Beobachtungsauftrag der Verfassungsschutzbehörden? In: Polizei-Führungsakademie Münster (Hrsg.), Aktuelle Rechtsprobleme im Zusammenhang mit der Bekämpfung der Organisierten Kriminalität. Schlussbericht über das Seminar 2000, S. 325–336 [zit.: *Forster,* in: Polizei-Führungsakademie Münster].

Fredman, Jonathan, Intelligence Agencies, Law Enforcement, and the Prosecution Team. Yale L. & Pol'y Rev. (16) 1998, S. 331–371.

Freyschmidt, Uwe/Ignor, Alexander, Mehr Verteidigung im Ermittlungsverfahren?! Anmerkungen zum Diskussionsentwurf für eine Reform des Strafverfahrens. NStZ 2004, S. 465–469.

Frister, Helmut, Das Gesetzesvorhaben der Bundesregierung zur Einführung des großen Lauschangriffs. StV 1996, S. 454–457.

– Der (bayrische) Verfassungsschutz als Strafverfolgungsbehörde? In: Joachim Schulz/Günter Bemmann (Hrsg.), Festschrift für Günter Bemmann. Zum 70. Geburtstag am 15. Dezember 1997. Baden-Baden 1997, S. 542–559.

Fromm, Heinz, Auftrag und Profil des Verfassungsschutzes im Zeichen neuer Bedrohungen. In: Bundesamt für Verfassungsschutz (Hrsg.), Terrorismusbekämpfung in Europa – Herausforderung für die Nachrichtendienste – Symposium, Vorträge auf dem 7. Symposium des Bundesamtes für Verfassungsschutz am 8. Dezember 2008. Köln 2008, S. 51–57 [zit.: *Fromm,* in: Bundesamt für Verfassungsschutz].

Gaede, Karsten, Die besonders vorsichtige Beweiswürdigung bei der exekutiven Sperrung von Beweismaterial im Konflikt mit dem Offenlegungsanspruch des Art. 6 I 1 EMRK. StraFo 2004, S. 195–198.

– Schranken des fairen Verfahrens gemäß Art. 6 EMRK bei der Sperrung verteidigungsrelevanter Informationen und Zeugen. StV 2006, S. 599–607.

Gärditz, Klaus, Strafprozeß und Prävention. Entwurf einer verfassungsrechtlichen Zuständigkeits- und Funktionenordnung. Tübingen 2003.

Gärditz, Klaus/Orth, Johannes, Geheimnisschutz im Verwaltungsprozess. JuS 2010, S. 317–321.

Gehring, Ingo, „Innere Sicherheit – USA". Rechtsvergleich der Entwicklung, Organisation, Aufgaben der Polizei und deren Kompetenzen – Systemtauglichkeit für Europa. Würzburg 1999.

Geiger, Andreas, Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung. NVwZ 1989, S. 35–38.

Genz, Alexander, Datenschutz in Europa und den USA. Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung. Wiesbaden 2004.

Gitenstein, Mark, Nine Democracies and the Problems of Detention, Surveillance, and Interrogation. In: Benjamin Wittes (Hrsg.), Legislating the War on Terror. An Agenda for Reform. Washington 2009, S. 7–42 [zit.: *Gitenstein,* in: Wittes].

Glaser, Michael/Gedeon, Bertolt, Dissonante Harmonie: Zu einem zukünftigen „System" strafprozessualer verdeckter Ermittlungsmaßnahmen. GA 2007, S. 415–436.

Gleß, Sabine, Zur „Beweiswürdigungs-Lösung" des BGH. NJW 2001, S. 3606–3607.

– Beweisrechtsgrundsätze einer grenzüberschreitenden Strafverfolgung. Baden-Baden 2006.

Glick, Scott, FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security. Harv. NSJ (1) 2010, S. 87–143.

Gola, Peter/Schomerus, Rudolf, BDSG. Bundesdatenschutzgesetz. 10. Aufl. München 2010 [zit.: BDSG].

Goldstein, Joseph, Police Discretion not to Involve the Criminal Process: Low Visibility Decisions in the Administration of Justice. Yale L.J. (69) 1960, S. 543–594.

Gössel, Karl, Zuständigkeit für Sperrerklärung. NStZ 1996, S. 287–289.

Graf, Jürgen Peter, Beck'scher Online-Kommentar. StPO, Stand: 1.2.2012, 13. Edition [zit.: Graf-*Bearbeiter*].

Grafe, Adina, Die Auskunftserteilung über Verkehrsdaten nach §§ 100g, 100h StPO. Staatliche Kontrolle unter Mitwirkung Privater. Freiburg 2007.

Graulich, Kurt, Justizgewährung und Geheimdienste. Einleitung. In: Kurt Graulich/Dieter Simon (Hrsg.), Terrorismus und Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Perspektiven. Berlin 2007, S. 143–163 [zit.: *Graulich,* in: Graulich/Simon].

Grawe, Stefan, Die strafprozessuale Zufallsverwendung. Zufallsfunde und andere Zweckdivergenzen bei der Informationsverwendung im Strafverfahren. Tübingen 2008.

Griesbaum, Rainer, Zum Verhältnis von Strafverfolgung und Gefahrenabwehr vor dem Hintergrund der Bedrohung durch den internationalen islamistischen Terrorismus. In: Rainer Griesbaum/Rolf Hannich/Karl Heinz Schnarr (Hrsg.), Strafrecht und Justizgewährung. Festschrift für Kay Nehm zum 65. Geburtstag. Berlin 2006, S. 125–137.

Grimmett, Richard, Authorization For Use Of Military Force in Response to the 9/11 Attacks (P.L. 107–40): Legislative History. CRS 16. Januar 2007, RS22357, S. 1–6.

Gröger, Annika, Das Akteneinsichtsrecht im Strafverfahren unter der besonderen Berücksichtigung der Europäischen Menschenrechtskonvention. Zugleich eine rechtsvergleichende Untersuchung zum französischen Recht. Hamburg 2009.

Gröpl, Christoph, Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung. Legitimation, Organisation und Abgrenzungsfragen. Berlin 1993.

– Vorläufige Einschränkung der Verwertungs- und Übermittlungsbefugnisse des Bundesnachrichtendienstes bei der strategischen Fernmeldeüberwachung. NJW 1996, S. 100–102.

Großkopf, Philipp, Beweissurrogate und Unmittelbarkeit der Hauptverhandlung. Zulässigkeit des Transfers von Vernehmungsergebnissen aus dem Ermittlungsverfahren in die Hauptverhandlung. Baden-Baden/Zürich 2007.

Grunwald, Anne, Datenerhebung durch das Federal Bureau of Investigation. Maßnahmen zur Terrorismusbekämpfung nach dem 11. September 2001. Baden-Baden 2008.

Grünwald, Gerald, Beweisverbote und Verwertungsverbote im Strafverfahren. JZ 1966, S. 489–501.

Gurulé, Jimmy/Corn, Geoffrey, Principles of Counter-Terrorism Law. St. Paul 2011.

Gusy, Christoph, Die Verwendung rechtmäßig erlangter Information durch die Nachrichtendienste. NVwZ 1983, S. 322–328.

– Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten. ZRP 1987, S. 45–52.

– Polizei und Nachrichtendienste im Kampf gegen die Organisierte Kriminalität. KritV 1994, S. 242–251.

– Beobachtung Organisierter Kriminalität durch den Verfassungsschutz? StV 1995, S. 320–326.

– Verfassungsfragen vorbeugenden Rechtsschutzes. JZ 1998, S. 167–174.

– Organisierte Kriminalität zwischen Polizei und Verfassungsschutz. GA 1999, S. 319–331.

– Geheimdienstliche Aufklärung und Grundrechtsschutz. Aus Politik und Zeitgeschichte 2004, S. 14–20.

– Parlamentarische Kontrolle der Nachrichtendienste im demokratischen Rechtsstaat. ZRP 2008, S. 36–40.

– Grundrechte und Verfassungsschutz. Wiesbaden 2011 [zit.: *Gusy,* Grundrechte].

– Polizei- und Ordnungsrecht. 8. Aufl.. Tübingen 2011 [zit.: *Gusy,* Polizeirecht].

– Reform der Sicherheitsbehörden. ZRP 2012, S. 230–234.

Haas, Günter, Vorermittlungen und Anfangsverdacht. Berlin 2003.

Hall, Matthew, Constitutional Regulation of National Security Investigation: Minimizing the Use of Unrelated Evidence. Wake Forest L. Rev. (41) 2006, S. 61–122.

Hamacher, Rolfjosef, Der heimliche Kontenzugriff und das Grundgesetz – Finanzbehörden als Geheimdienst? DStR 2006, S. 633–638.

Hamm, Rainer, Verwertung rechtswidriger Ermittlungen – nur zugunsten des Beschuldigten? StV 1998, S. 361–366.

Hardin, David, Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA under the Fourth Amendment. Geo. Wash. L. Rev. (71) 2003, S. 291–346.

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

Harris, Grant, The CIA Mandate and the War on Terror. Yale L. & Pol'y Rev. (23) 2005, S. 529–576.

Hay, Peter, US-Amerikanisches Recht. Ein Studienbuch. 4. Aufl. München/Wien 2008.

Hefendehl, Roland, Die neue Ermittlungsgeneralklausel der §§ 161, 163 StPO: Segen oder Fluch? StV 2001, S. 700–706.

– Die Entfesselung des Strafverfahrens über Methoden der Nachrichtendienste. Bestandsaufnahme und Rückführungsversuch. GA 2011, S. 209–231.

Heghmanns, Michael, Heimlichkeit von Ermittlungshandlungen. In: Henning Müller/Günther M. Sander/Helena Válková (Hrsg.), Festschrift für Ulrich Eisenberg zum 70. Geburtstag. München 2009.

Heine, Günter, Beweisverbote und Völkerrecht: Die Affäre Liechtenstein in der Praxis. HRRS 2009, S. 540–547.

Hellmann, Uwe, Strafprozessrecht. 2. Aufl. Berlin 2006.

Herrmann, Joachim, Die Reform der deutschen Hauptverhandlung nach dem Vorbild des anglo-amerikanischen Strafverfahrens. Bonn 1971 [zit.: *Herrmann*, Reform].

– Aufgaben und Grenzen der Beweisverbote. Rechtsvergleichende Überlegungen zum deutschen und amerikanischen Recht. In: Theo Vogler (Hrsg.), Festschrift für Hans-Heinrich Jescheck zum 70. Geburtstag. Berlin 1985, S. 1291–1310.

Hilger, Hans, Neues Strafverfahrensrecht durch das OrgKG. 1. Teil. NStZ 1992, S. 457–463.

Hirsch, Alexander, Die Kontrolle der Nachrichtendienste. Vergleichende Bestandsaufnahme, Praxis und Reform. Berlin 1996.

Hitz, Frederick, Unleashing the Rogue Elephant: September 2011 and Letting the CIA be the CIA. Harv. J. L. & Pub. Pol'y (25) 2002, S. 765–780.

Hochreiter, Monika, Die heimliche Überwachung internationaler Telekommunikation: Eine rechtsvergleichende Untersuchung zur Rechtsstaatlichkeit der Arbeit von Auslandsnachrichtendiensten in Deutschland und dem Vereinigten Königreich unter besonderer Berücksichtigung der Europäischen Menschenrechtskonvention. München 2002.

Holzer, Rachel, National Security Versus Defense Counsel's "Need to Know": An Objective Standard for Resolving the Tension. Fordham L. Rev. (73) 2005, S. 1941–1986.

Hooper, Laural/Rauma, David/Leary, Marie/Thrope, *Shelia*, A Summary of Responses to a National Survey of Rule 16 of the Federal Rules of Criminal Procedure and Disclosure Practices in Criminal Cases. Final Report to the Advisory Committee on Criminal Rules 2011 [abrufbar unter: www.uscourts.gov/uscourts/RulesAndPolicies/rules/Publications/Rule16Rep.pdf; Stand: 1.5.2012].

Hörauf, Dominic, Die demokratische Kontrolle des Bundesnachrichtendienstes. Ein Rechtsvergleich vor und nach 9/11. Hamburg 2011.

Howell, Beryl/Lesemann, Dana, FISA's Fruits in Criminal Cases: An Opportunity for Improved Accountability. UCLA J. Int'l L. & For. Aff. (145) 2007, S. 145–162.

Huber, Bertold, Das neue G 10-Gesetz. NJW 2001, S. 3296–3302.

– Das Bankgeheimnis der Nachrichtendienste. Zur Neuregelung der Auskunftsersuchen der Nachrichtendienste durch das Terrorismusbekämpfungsergänzungsgesetz vom 9.1.2007. NJW 2007, S. 881–883.

– Die Reform der parlamentarischen Kontrolle der Nachrichtendienste und des Gesetzes nach Art. 10 GG. NVwZ 2009, S. 1321–1328.

– Ein Europäischer Nachrichtendienst? 6. Konferenz der Parlamentarischen Kontrollausschüsse vom 29. 9. bis 1.10.2010 in Brüssel. NVwZ 2011, S. 409–412.

Hulnick, Arthur, Home Time: A New Paradigm for Domestic Intelligence. IJIC (22) 2009, S. 569–585.

Hund, Horst, Polizeiliches Effektivitätsdenken contra Rechtsstaat. ZRP 1991, S. 463–468.

Imle, Walter, Zwischen Vorbehalt und Erfordernis. Eine historische Studie zur Entstehung des nachrichtendienstlichen Verfassungsschutzes nach 1945. München 1984.

Innenministerium des Landes Nordrhein-Westfalen, Verfassungsschutz in Nordrhein-Westfalen [abrufbar unter: www.im.nrw.de/imshop/shopdocs/Verfassungsschutz_in_NRW.pdf; Stand: 1.5.2012; zit.: Innenministerium des Landes Nordrhein-Westfalen].

Isenberg, David, The Pitfalls of U.S. Covert Operations. Cato Policy Analysis (118) 1989, S. 1–20.

Jäger, Thomas/Daun, Anna, Die Koordination der Nachrichtendienste im Ländervergleich: USA, Großbritannien, Frankreich, Deutschland, Schweden, Australien und Kanada. In: Heiko Borchert (Hrsg.), Verstehen, dass die Welt sich verändert hat. Neue Risiken, neue Anforderungen und die Transformation der Nachrichtendienste. Baden-Baden 2005, S. 57–76 [zit.: *Jäger/Daun,* in: Borchert].

Joecks, Wolfgang, Studienkommentar StPO. 3. Aufl. München 2011 [zit.: *Joecks*].

Johnson, Elizabeth, Surveillance and Privacy Under the Obama Administration: The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 and the *Attorney General's* Guidelines for Domestic FBI Operations. I/S: J.L. & Pol'y for Info. Soc'y (5:3) 2010, S. 419–446.

Jones, Allison, The 2008 Guidelines: Contradiction of Original Purpose. B.U. Pub. Int. L.J. (19) 2008, S. 137–174.

Julius, Karl-Peter, Strafprozessordnung. 4. Aufl. Heidelberg 2009 [zit.: Julius-*Bearbeiter*].

Karlsruher Kommentar zur Strafprozessordnung. Mit GVG, EGGVG und EMRK. Hrsg. von Rolf Hannich. 6. Aufl. München 2008 [zit.: KK-*Bearbeiter*].

Kamisar, Yale/LaFave, Wayne/Israel, Jerold/King, Nancy J./Kerr, Orin S., Modern Criminal Procedure. Cases, Comments and Questions. 12. Aufl. St. Paul 2008.

Keller, Rolf/Griesbaum, Rainer, Das Phänomen der vorbeugenden Bekämpfung von Straftaten. NStZ 1990, S. 416–420.

Kelnhofer, Evelyn/Krug, Björn, Der Fall LGT Liechtenstein – Beweisführung mit Material aus Straftaten im Auftrag des deutschen Fiskus? StV 2008, S. 660–668.

Kerr, Orin, The Modest Role of the Warrant Clause in National Security Investigations. Tex. L. Rev. (88) 2010, S. 1669–1684.

Kilian, Wolfang/Heussen, Benno, Computerrechts-Handbuch. 29. Ergänzungslieferung. München 2011 [zit.: Kilian/Heussen-*Bearbeiter*].

Kibbe, Jennifer, Covert Action and the Pentagon. Intelligence and National Security (22:1) 2007, S. 57–74.

King, Matthew, Security, Scale, Form, and Function: The Search for Truth and the Exclusion of Evidence in Adversarial and Inquisitorial Justice Systems. Int'l Legal Persp. (12) 2002, S. 185–236.

Kistner-Bahr, Hanna, Die Entwicklungstendenzen Europols im europäischen Integrationsprozess. Mögliche Ausweitung der Befugnisse Europols vom Informationsaustausch zur Ermittlungskompetenz unter Berücksichtigung des Vertrages von Lissabon. Köln 2010.

Klee, Reinhard, Neue Instrumente der Zusammenarbeit von Polizei und Nachrichtendiensten. Geltung, Rang und Reichweite des Trennungsgebots. Baden-Baden 2010.

Knieriem, Thomas, Fallrepetitorium zur Telekommunikationsüberwachung nach neuem Recht. StV 2008, S. 599–606.

Koch, Martin, Überwachung der Organisierten Kriminalität durch den bayerischen Verfassungsschutz. ZRP 1995, S. 24–28.

König, Marco, Trennung und Zusammenarbeit von Polizei und Nachrichtendiensten. Schriften zum Recht der inneren Sicherheit, Bd. 7. Stuttgart 2005.

Kornblum, Thorsten, Rechtsschutz gegen geheimdienstliche Aktivitäten. Schriften zum Öffentlichen Recht, Bd. 1174. Berlin 2010.

Korte, Guido, Die Informationsgewinnung der Nachrichtendienste mit nachrichtendienstlichen Mitteln. Grenzen und Möglichkeiten der Informationsbeschaffung durch die Verfassungsschutzbehörden. In: Guido Korte/Manfred Zoller (Hrsg.), Informationsgewinnung mit nachrichtendienstlichen Mitteln, Rahmenbedingungen, Einsatzmodalitäten, Verarbeitungsaspekte. Brühl/Rheinland 2001, S. 35–87 [zit.: *Korte*, in: Korte/Zoller].

Kosar, Kevin, Classified Information Policy and Executive Order 13526. CRS 10. Dezember 2010, R41528, S. 1–19.

Kramer, Bernhard, Die Beschlagnahmefähigkeit von Behördenakten im Strafverfahren. NJW 1984, S. 1502–1506.

– Grundbegriffe des Strafverfahrensrechts. 6. Aufl. Stuttgart 2004.

Krekeler, Wilhelm/Löffelmann, Markus/Sommer, Ulrich, Strafprozessordnung. 2. Aufl. Bonn 2010 [zit.: Krekeler/Löffelmann-*Bearbeiter*].

Kretschmer, Joachim, BKA, BND und BfV – was ist das und was dürfen die? JURA 2006, S. 336–343.

Kris, David, Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come. In: Benjamin Wittes (Hrsg.), Legislating the War on Terror. An Agenda for Reform. Washington. DC 2009, S. 217–251 [zit.: *Kris,* in: Wittes].

– Law Enforcement as a Counterterrorism Tool. J. Nat'l Sec. L. & Pol'y (5) 2011, S. 2–95.

Kris, David S./Wilson, J. Douglas, National Security Investigations and Prosecutions. Vol. 1 and 2. 2nd ed. Eagan, Minn. 2012.

Krüßmann, Thomas, Transnationales Strafprozessrecht. Baden-Baden 2009.

Kuhlmann, Axel, Terroristische Netzwerke. Bekämpfung in Netzwerken. In: Guido Korte (Hrsg.), Aspekte der nachrichtendienstlichen Sicherheitsarchitektur. Brühl/Rheinland 2005, S. 111–208 [zit.: *Kuhlmann,* in: Korte].

Kuhn, Bernd, Die Widerspruchslösung. JA 2010, S. 891–893.

Kühne, Hans-Heiner, Strafprozessrecht. Eine systematische Darstellung des deutschen und europäischen Strafverfahrensrechts. 8. Aufl. Heidelberg 2010 [zit.: *Kühne*, Strafprozessrecht].

– Die Verwertbarkeit von illegal erlangten Steuerdaten im Strafverfahren – Zugleich eine Stellungnahme zum Beschluss des BVerfG vom 9.11.2010. In: Manfred Heinrich/Christian Jäger/Hans Achenbach (Hrsg.), Strafrecht als Scientia Universalis. Festschrift für Claus Roxin zum 80. Geburtstag am 15. Mai 2011. Berlin 2011, S. 1269–1286.

Kutscha, Martin, Neue Grenzmarken des Polizeiverfassungsrechts. NVwZ 2005, S. 1231–1234.

– Innere Sicherheit und Verfassung. In: Fredrik Roggan/Martin Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit. Berlin 2006, S. 24–104 [zit.: *Kutscha,* in: Roggan/Kutscha].

– Die Antinomie des Verfassungsschutzes. NVwZ 2013, S. 324–327.

Lange, Nicole, Vorermittlungen. Die Behandlung des staatsanwaltschaftlichen Vorermittlungsverfahrens unter besonderer Berücksichtigung von Abgeordneten, Politikern und Prominenten. Frankfurt a.M./New York 1999.

– Staatsanwaltschaftliche Vorermittlungen – ohne rechtliche Grundlage? DRiZ 2002, S. 264–273.

Lepsius, Oliver, Verwaltungsrecht unter dem Common Law. Amerikanische Entwicklungen bis zum New Deal. Tübingen 1997.

Linke, Heinz-Dieter, Das Zollkriminalamt. Eine geheimnisvolle, unsichtbare und mächtige Strafverfolgungsbehörde? Frankfurt a.M. u.a. 2004.

Lisken, Hans, Polizei und Verfassungsschutz: Aspekte der gesetzlichen Zusammenarbeit. NJW 1982, S. 1481–1488.

– Sperrerklärung im Strafprozess. NJW 1991, S. 1658–1660.

– „V-Leute“ im Verfassungsprozess. ZRP 2003, S. 45–48.

Lisken, Hans/Denninger, Erhard, Die Polizei im Verfassungsgefüge. In: Hans Lisken/Erhard Denninger/Frederik Rachor (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr, Strafverfolgung, Rechtsschutz. 4., neu bearb. u. erw. Aufl. München 2007, S. 67–150 [zit.: *Lisken/Denninger,* in: Lisken/Denninger/Rachor].

Litt, Robert/Bennett, Wells, Better Rules for Terrorism Trials. In: Benjamin Wittes (Hrsg.), Legislating the War on Terror. An Agenda for Reform. Washington, DC 2009, S. 142–179 [zit.: *Litt/Benett,* in: Wittes].

Liu, Edward, Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015. CRS 16. Januar 2011, R40138, S. 1–14.

Liu, Edward/Garvey, Todd, Protecting Classified Information and the Rights of Criminal Defendants: The Classified Information Procedures Act. CRS 2. April 2012, R41742, S. 1–12.

Logan, Cedric, The FISA Wall and Federal Investigations. N.Y.U. J.L. & Liberty (4) 2009, S. 209–251.

Lohberger, Ingram, Mittelbare Verwertung sog. Zufallserkenntnisse bei rechtmäßiger Telefonüberwachung nach §§ 100a, b StPO? In: Udo Ebert (Hrsg.), Festschrift für Ernst-Walter Hanack zum 70. Geburtstag am 30. August 1999. Berlin 1999, S. 253–276.

Löwe, Ewald/Rosenberg, Werner/Erb, Volker/Franke, Ulrich, Die Strafprozessordnung und das Gerichtsverfassungsgesetz. 25. Aufl. Berlin 1997–2005, sowie 26. Aufl. Berlin 2007 [zit.: Löwe/Rosenberg-*Bearbeiter*].

Lüderssen, Klaus, Zur „Unerreichbarkeit" des V-Mannes. In: Günter Kohlmann (Hrsg.), Festschrift für Ulrich Klug zum 70. Geburtstag. Bd. II. Köln 1983, S. 527–538.

Lundberg, David, Democratic Accountability of the United States Intelligence Community. In: Daniel Baldino (Hrsg.), Democratic oversight of intelligence services. Annandale New South Wales 2010, S. 59–82 [zit.: *Lundberg*, in: Baldino].

Maggs, Gregory, Terrorism and the Law. Cases and Materials. 2. Aufl. St. Paul 2010.

Mahler, Franziska, Das Recht des Beschuldigten auf konfrontative Befragung der Belastungszeugen. Eine vergleichende Analyse der normativen und justiziellen Vorgaben für das Konfrontationsrecht im US-amerikanischen, europäischen und deutschen Strafverfahrensrecht. Frankfurt 2011.

Manget, Fred, Intelligence and the Criminal Law System. Stan. L. & Pol'y Rev. (17) 2006, S. 415–435.

Margedant, Jochen, Das „in camera"-Verfahren. NVwZ 2001, S. 759–764.

Markwordt Skehan, Anja, Die Einleitung der Untersuchungshaft. Eine rechtsvergleichende Studie zur Inhaftierung des Verdächtigen im Vorverfahren in Deutschland und den USA. Unter besonderer Berücksichtigung der Rechtssysteme der US-Bundesstaaten Kalifornien, Texas und New York. Göttingen 2011.

Martin, Kate, Domestic Intelligence and Civil Liberties. SAIS Review (24) 2004, S. 7–21.

Masse, Todd, The FBI: Past, Present, and the Future. CRS 2. Oktober 2003, RL32095, S. 1–46.

– Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches. CRS 18. August 2006, RL33616, S. 1–23.

Maunz, Theodor/Dürig, Günter/Herzog, Roman, Kommentar zum Grundgesetz. Loseblattsammlung, Stand: 63. Ergänzungslieferung. München 2011 [zit.: Maunz/Dürig-*Bearbeiter*].

Maurer, Hartmut, Allgemeines Verwaltungsrecht. 18. Aufl. München 2011.

Maxwell, K. C./Cline, John, Criminal Prosecution and Classified Information. Los Angeles Lawyer (29) 2006, S. 35–43.

McCarthy, Andrew, Why Section 218 Should be Retained 2005 [abrufbar unter: http://apps.americanbar.org/natsecurity/patriotdebates/218–2#opening; Stand: 1.5.2012].

McCarthy, Michael, Recent Developments. USA Patriot Act. Harv. J. Leg. (39) 2002, S. 435–453.

McNamara, Robert, A Primer on the Changing Role of Law Enforcement and Intelligence in the War on Terrorism. In: Markle Foundation (Hrsg.), Protecting America's Freedom in the Information Age. New York City 2002, S. 81–92 [abrufbar unter: http://

www.markle.org/publications/667-protecting-americas-freedom-information-age; Stand: 1.5.2012; zit.: *McNamara,* in: Markle Foundation].

Meier, Bernd-Dieter, Richtervorbehalt bei der Blutprobe: Verzichtbare Belastung aller Verfahrensbeteiligten? ZRP 2010, S. 223–226.

Meyer, Aric, FISA and Warrantless Wire-Tapping: Does FISA Conform to Fourth Amendment Standards? 2009 [abrufbar unter: http://digital.library.unt.edu/ark:/67531/metadc9838/m1/1/high_res_d/thesis.pdf; Stand: 1.5.2012].

Meyer, Jürgen, Urteilsanmerkung zum BGH Urteil vom 14.11.1984 – 3 StR 418/84. NStZ 1986, S. 132–133.

Meyer-Goßner, Lutz/Cierniak, Jürgen, Strafprozessordnung. Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen. München 2009.

Mosbacher, Andreas, Aktuelles Strafprozessrecht. JuS 2007, S. 724–728.

Müller, Egon, Strafverteidigung. NJW 1981, S. 1801–1807.

Müller, Henning, Behördliche Geheimhaltung und Entlastungsvorbringen des Angeklagten. Tübingen 1992 [zit.: *H. Müller*, Geheimhaltung].

– Urteilsanmerkung zum BGH Urteil vom 4.3.2004. JZ 2004, S. 926–928.

Münchener Kommentar zum Strafgesetzbuch. Bd. 3: §§ 80–184g StGB. Hrsg. von Klaus Miebach, München 2012 [zit.: MüKoStGB-*Bearbeiter*].

Nack, Armin, Verwertung rechtswidriger Ermittlungen nur zugunsten des Beschuldigten? StV 1998, S. 366–373.

Nagler, Axel, Erfahrungsbericht aus einem durchprozessierten Verfahren nach § 129b StGB – Al Queda. In: Baden-Württembergische Strafverteidiger e.V. (Hrsg.), Heimlichkeit und Wahrheit. Die neuen Maximen des Strafprozesses; 32. Strafverteidigertag München 29.2.–2.3.2008. Berlin 2009, S. 153–180 [zit.: *Nagler,* in: Baden-Württembergische Strafverteidiger e.V.].

Nehm, Kay, Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur. NJW 2004, S. 3289–3295.

– Die Zuständigkeit des Generalbundesanwalts für die Verfolgung extremistischer Einzeltäter. München 2002 [zit.: *Nehm*, Zuständigkeit].

Norouzi, Ali, Videovernehmung unter optisch-akustischer Abschirmung – BGH. NJW 2003, 74, JuS 2003, S. 434–438.

Oaks, Dallin, Studying the Exclusionary Rule in Search and Seizure. U. Chi. L. Rev. (37) 1970, S. 665–757.

Office of the Attorney General, The Attorney General's Guidelines for Domestic FBI Operations 2008 [abrufbar unter: http://www.justice.gov/ag/readingroom/guidelines.pdf; Stand: 1.5.2012; zit.: Mukasey Guidelines 2008].

Office of the Director of National Intelligence, An Overview of the United States Intelligence Community for the 111th Congress [abrufbar unter: http://dni.gov/overview.pdf; Stand: 1.5.2012; zit.: ODNI zur IC 2009].

Office of the Director of National Intelligence, National Intelligence: a consumer's guide 2009 [abrufbar unter: http://dni.gov/IC_Consumers_Guide_2009.pdf; Stand: 1.5.2012; zit.: ODNI Guide 2009].

Ortiz, Daniel, Legal Authorities for "All-Source" Domestic Intelligence. In: Markle Foundation (Hrsg.), Protecting America's Freedom in the Information Age. New York 2002, S. 93–100 [zit.: *Ortiz,* in: Markle Foundation].

Ossenberg, Sarah, Die Fernwirkung im deutsch-U.S.-amerikanischen Vergleich. Unter besonderer Berücksichtigung der Funktionen der Beweisverwertungsverbote. Schriftenreihe zum internationalen Einheitsrecht und zur Rechtsvergleichung, Bd. 22. Hamburg 2011.

Ostendorf, Heribert, Gekaufte Strafverfolgung. Die Strafbarkeit des Erwerbs von „geklauten" Steuerdaten und ihre Beweisverwertung. ZIS 2010, S. 301–308.

Ostheimer, Michael, Verfassungsschutz nach der Wiedervereinigung. Möglichkeiten und Grenzen einer Aufgabenausweitung. Frankfurt a.M./New York 1994.

Paeffgen, Hans-Ulrich, Kompetenzen zur (präventiven und repressiven) Datenübermittlung. In: Jürgen Wolter/Wolf-Rüdiger Schenke/Peter Rieß/Mark Zöller (Hrsg.), Datenübermittlungen und Vorermittlungen: Festgabe für Hans Hilger. Heidelberg 2003, S. 153–170.

Pawlik, Michael, Zur strafprozessualen Verwertbarkeit rechtswidrig erlangter ausländischer Bankdaten. JZ 2010, S. 693–702.

Peitsch, Dietmar/Polzin, Christina, Die parlamentarische Kontrolle der Nachrichtendienste. NVwZ 2000, S. 387–393.

Pelz, Christian, Beweisverwertungsverbote und hypothetische Ermittlungsverläufe. München 1993.

Perez, Evan, Rights Are Curtailed for Terror Suspects. The Wall Street Journal vom 24.3.2011 [abrufbar unter: http://online.wsj.com/article/SB10001424052748704050204576218970652119898.html?mod=wsj_share_twitter; Stand: 1.5.2012].

Perron, Walter, Das Beweisantragsrecht des Beschuldigten im deutschen Strafprozess. Eine Untersuchung der verfassungsrechtlichen und verfahrensstrukturellen Grundlagen, gesetzlichen Regelungen und rechtstatsächlichen Auswirkungen sowie eine Erörterung der Reformperspektiven unter rechtsvergleichender Berücksichtigung des adversatorischen Prozessmodells. Berlin 1995 [zit.: *Perron,* Beweisantragsrecht].

– Rechtsvergleichender Querschnitt und rechtspolitische Bewertung. In: Walter Perron (Hrsg.), Die Beweisaufnahme im Strafverfahrensrecht des Auslands. Rechtsvergleichendes Gutachten. Freiburg 1995, S. 549–608 [zit.: *Perron,* in: ders.].

Peters, Karl, Fehlerquellen im Strafprozeß. Eine Untersuchung der Wiederaufnahmeverfahren in der Bundesrepublik Deutschland. Bd. 2: Systematische Untersuchungen und Folgerungen. Karlsruhe 1972.

Pfeiffer, Christian, Telefongespräche im Visier der elektronischen Rasterfahndung. ZRP 1994, 253–255.

Pfeiffer, Gerd, Strafprozessordnung. Kommentar. 5. Aufl. München 2005 [zit.: *Pfeiffer* StPO].

Pieroth, Bodo/Schlink, Bernhard/Kniesel, Michael, Polizei- und Ordnungsrecht. 6. Aufl. München 2010.

Posner, Richard, Remaking Domestic Intelligence. Stanford, California, 2005.

Puschke, Jens/Singelnstein, Tobias, Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1.1.2008. NJW 2008, S. 113–119.

Rackow, Sharon, How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of Intelligence Investigations. U. Pa. L. Rev. (150) 2002, S. 1651–1696.

Radtke, Henning/Hohmann, Olaf, Strafprozessordnung (StPO). Kommentar. München 2011 [zit.: Radtke/Hohmann-*Bearbeiter*].

Rascoff, Samuel, Domesticating Intelligence. S. Cal. L. Rev. (83) 2010, S. 575–648.

Rebmann, Kurt, Der Zeuge vom Hörensagen im Spannungsverhältnis zwischen gerichtlicher Aufklärungspflicht, Belangen der Exekutive und Verteidigungsinteressen. NStZ 1982, S. 315–321.

Reese, Mary, Organisation Gehlen. Der Kalte Krieg und der Aufbau des deutschen Geheimdienstes. Berlin 1992.

Rehbein, Mareike, Die Verwertbarkeit von nachrichtendienstlichen Erkenntnissen aus dem In- und Ausland im deutschen Strafprozess. Berlin 2011.

Reilly, Ryan, New Guidance Allows FBI to Delay Reading Miranda Rights to Terror Suspects. TPM vom 24.3.2011 [abrufbar unter: http://tpmmuckraker.talkingpointsmemo.com/2011/03/new_guidance_allows_fbi_to_delay_reading_miranda_rights_to_terror_suspects.php; Stand: 1.5.2012].

Reinbacher, Tobias, Das Strafrechtssystem der USA. Eine Untersuchung zur Strafgewalt im föderativen Staat. Berlin 2010.

Remmele, Wolf-Dieter, Die Beobachtung der Organisierten Kriminalität – eine Aufgabe für den Verfassungsschutz. In: Bundesministerium des Inneren (Hrsg.), Verfassungsschutz: Bestandsaufnahme und Perspektiven. Bonn 1998, S. 312–337 [zit.: *Remmele,* in: Bundesministerium des Inneren].

Rheinstein, Max/Borries, Reimer von/Niethammer, Hans-Eckart, Einführung in die Rechtsvergleichung. 2. Aufl. München 1987.

Riegel, Reinhard, Informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden (I). Vorschläge für eine gesetzliche Regelung der Tätigkeit des Bundesnachrichtendienstes. Computer und Recht 1986, S. 343–352.

– Der Quantensprung des Gesetzes zu Art. 10 GG (G10). ZRP 1995, S. 176–180.

Rieger, Thomas, Nachrichtendienst und Rechtsstaat. ZRP 1985, S. 3–11.

Rieß, Peter, Datenübermittlungen im neuen Strafprozessrecht. In: Jürgen Wolter/Wolf-Rüdiger Schenke/Peter Rieß/Mark Zöller (Hrsg.), Datenübermittlungen und Vorermittlungen: Festgabe für Hans Hilger. Heidelberg 2003, S. 171–181.

Roach, Kent, The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation between Intelligence and Evidence 2010 [abrufbar unter: http://ssrn.com/abstract=1629227; Stand: 1.5.2012; zit.: *Roach,* Challenges].

Roach, Kent, The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence. In: Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Hrsg.), Research papers. Ottawa 2010, S. 311–394 [zit.: *Roach,* in: Commission of Inquiry].

Robbers, Gerhard, Der Grundrechtsverzicht. JuS, 1985, S. 925–931.

Rödder, Markus, Verfassungsschutz im föderalen Gefüge der Bundesrepublik Deutschland. Bonn 2010.

Roewer, Helmut, Nachrichtendienstrecht der Bundesrepublik Deutschland. Kommentar und Vorschriftensammlung für die Praxis der Verfassungsschutzbehörden, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes. Köln 1987.

Rogall, Klaus, Informationseingriff und Gesetzesvorbehalt im Strafprozess. ZStW 103 (1991), S. 907–956.

– Beweisverbote im System des deutschen und des amerikanischen Strafverfahrens. In: Jürgen Wolter (Hrsg.), Zur Theorie und Systematik des Strafprozeßrechts. Neuwied u.a., 1995, S. 113–160 [zit.: *Rogall,* in: Wolter].

– Über die Folgen der rechtswidrigen Beschaffung des Zeugenbeweises im Strafprozeß. JZ 1996, S. 944–955.

– Das Verwendungsverbot des § 393 II AO. In: Hans Joachim Hirsch/Günter Kohlmann (Hrsg.), Festschrift für Günter Kohlmann zum 70. Geburtstag. Köln 2003, S. 465–498.

– Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus. JZ 2008, S. 818–830.

Roggan, Fredrik, Auf legalem Weg in einen Polizeistaat. Entwicklung des Rechts der Inneren Sicherheit. Bonn 2000 [zit.: *Roggan,* Polizeistaat].

– Mit Schlapphüten gegen die Mafia: OK-Beobachtung durch den Verfassungsschutz. Bürgerrechte & Polizei 2004, S. 35–39.

– Befugnisse im Polizei- und Strafprozessrecht. In: Fredrik Roggan/Martin Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit. Berlin 2006, S. 105–385 [zit.: *Roggan*, in: Roggan/Kutscha].

– Neue Aufgaben und Befugnisse im Geheimdienstrecht. In: Fredrik Roggan/Martin Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit. Berlin 2006, S. 411–444 [zit.: *Roggan,* in: Roggan/Kutscha].

– Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur. NJW 2009, S. 257–262.

– G-10-Gesetz. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. Baden-Baden 2012 [zit.: G10].

Roggan, Fredrik/Bergemann, Nils, Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland. Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz. NJW 2007, S. 876–881.

Romain, Alfred/Byrd, Sharon/Thielecke, Carola, Wörterbuch der Rechts- und Wirtschaftssprache. Bd. 2: deutsch-englisch. 4. Aufl. München 2002.

Rose-Stahl, Monika, Recht der Nachrichtendienste. 2. Aufl. Brühl/Rheinland 2006.

Ross, Jacqueline, The Elusive Line Between Prevention and Detection of Crime in German Undercover Policing. In: Markus Dirk Dubber (Hrsg.), Police and the Liberal State. Stanford, California, 2008, S. 136–156 [zit.: *Ross,* in: Dubber].

– Regulating Surveillance in America: the Emergence of Foreign Intelligence Investigations as Alternatives to the Criminal Process. Freiburg 2009 [zit.: *Ross,* Surveillance].

Roxin, Claus/Schäfer, Gerhard/Widmaier, Gunter, Die Mühlenteichtheorie. Überlegungen zur Ambivalenz von Verwertungsverboten. StV 2006, S. 655–661.

Roxin, Claus/Schünemann, Bernd, Strafverfahrensrecht. Ein Studienbuch. 27. Aufl. München 2012.

Rozen, Laura, Information Sharing at the FBI. In: Markle Foundation (Hrsg.), Protecting America's Freedom in the Information Age. New York 2002, S. 113–126 [zit.: *Rozen,* in: Markle Foundation].

Salditt, Franz, Herausforderung – aktuelle politische und andere Erwartungen an das Steuerstrafrecht. In: Wolfgang Spindler/Klaus Tipke/Thomas Rödder (Hrsg.), Steuerzentrierte Rechtsberatung. Festschrift für Harald Schaumburg zum 65. Geburtstag. Köln 2009, S. 1269–1287.

Salgado, Richard, Government Secrets, Fair Trials, and the Classified Information Procedures Act. Yale L. J. (98) 1988, S. 427–446.

Schaefer, Christoph, Strafverfolgung und Verfassungsschutz. NJW 1999, S. 2572–2573.

Schäfer, Gerhard/Wache, Volkhard/Meiborg, Gerhard, Gutachten zum Verhalten der Thüringer Behörden und Staatsanwaltschaften bei der Verfolgung des „Zwickauer Trios". Erfurt 14. Mai 2012.

Schäfer, Heike, Präventive Telekommunikationsüberwachung. Freiburg 2007.

Schafranek, Frank, Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland. Aachen 2000.

Schäuble, Wolfgang, Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts. ZRP 2007, S. 210–213.

Scheb, John/Scheb, John, II, An Introduction to the American Legal System. 2. Aufl. New York 2010.

Scheppele, Kim, We Are All Post–9/11 Now. Fordham L. Rev. (75) 2006, S. 607–630.

Schlegel, Stephan, Das Akteneinsichtsrecht des Beschuldigten im Strafverfahren. HRRS 2004, S. 411–417.

Schmitz, Christian, Die strafrichterliche Beweiswürdigung außerstrafrechtlicher Vorfragen, Hamburg. Köln 2011.

Schnabel, Christoph, Sperrerklärung zu Eichmann-Akten des Bundesnachrichtendienstes im verwaltungsgerichtlichen Verfahren rechtswidrig. NVwZ 2010, S. 881–883.

Schnarr, Karl, Zur Verknüpfung von Richtervorbehalt, staatsanwaltschaftlicher Eilanordnung und richterlicher Bestätigung. NStZ 1991, S. 209–216.

Schneider, Hans-Peter, Rechtsschutz und Verfassungsschutz. Zur Kontrolle nachrichtendienstlicher Tätigkeit durch Verwaltungsgerichte. NJW 1978, S. 1601–1605.

Schünemann, Bernd, Die Liechtensteiner Steueraffäre als Menetekel des Rechtsstaats. NStZ 2008, S. 305–310.

– Prolegomena zu einer jeden künftigen Verteidigung, die in einem geheimdienstähnlichen Strafverfahren wird auftreten können. GA 2008, S. 314–334.

Schwartz, Paul, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance. Hastings L. J. (54) 2003, S. 751–804.

Schwörer, Andreas, Die grenzüberschreitende Beweisnutzung im Abgabenverfahren und Steuerstrafverfahren bei hinzutretendem Wechsel der Verfahrensart. Norderstedt 2009.

Shea, Timothy, CIPA under Siege: The Use and Abuse of Classified Information in Criminal Trials. Am. Crim. L. Rev. (27) 1990, S. 657–716.

Sieber, Ulrich, Grenzen des Strafrechts. Grundlagen und Herausforderungen des neuen strafrechtlichen Forschungsprogramms am Max-Planck-Institut für ausländisches und internationales Strafrecht. ZStW 119 (2007), S. 1–68.

– Ermittlungen in Sachen Liechtenstein – Fragen und erste Antworten. NJW 2008, S. 881–886.

– Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt. Eine Analyse der Vorfeldtatbestände im „Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten". NStZ 2009, S. 353–364.

Signorelli, Walter, Criminal law, procedure, and evidence. Boca Raton, Florida, 2011.

Simitis, Spiros, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. NJW 1984, S. 394–405.

Singelnstein, Tobias, Strafprozessuale Verwendungsregelungen zwischen Zweckbindungsgrundsatz und Verwertungsverboten. Voraussetzungen der Verwertung von Zufallsfunden und sonstiger zweckentfremdender Nutzung personenbezogener Daten im Strafverfahren seit dem 1. Januar 2008. ZStW 120 (2008), S. 854–893.

Singer, Jens, Die rechtlichen Vorgaben für die Beobachtung der Organisierten Kriminalität durch die Nachrichtendienste der Bundesrepublik Deutschland. Aachen 2002 [zit.: *Singer*, OK].

– Das Trennungsgebot – Teil 1. Politisches Schlagwort oder verfassungsrechtliche Vorgabe? Die Kriminalpolizei 2006, S. 85–90.

– Das Trennungsgebot – Teil 2. Politisches Schlagwort oder verfassungsrechtliche Vorgabe? Die Kriminalpolizei 2006, S. 112–117.

– Nachrichtendienste zwischen innerer und äußerer Sicherheit. In: Thomas Jäger/Anna Daun (Hrsg.), Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009, S. 265–292 [zit.: *Singer,* in: Jäger/Daun].

Smith, Jeffrey/Howe, Elizabeth, Federal Constraints on Electronic Surveillance. In: Markle Foundation (Hrsg.), Protecting America's Freedom in the Information Age. New York 2002, S. 133–148.

Soiné, Michael, Die Aufklärung der Organisierten Kriminalität durch den Bundesnachrichtendienst. DöV 2006, S. 204–213.

– Erkenntnisverwertung von Informanten und V-Personen der Nachrichtendienste in Strafverfahren. NStZ 2007, S. 247–253.

– Aufklärung der Organisierten Kriminalität – (k)eine Aufgabe für Nachrichtendienste? ZRP 2008, S. 108–111.

– Kriminalistische List im Ermittlungsverfahren. NStZ 2010, S. 596–602.

Solove, Daniel, Digital Dossiers and the Dissipation of Fourth Amendment Privacy. S. Cal. L. Rev. 2002, S. 1083–1168.

Spaulding, Suzanna, If it ain't broke, don't fix it 2005 [abrufbar unter: http://apps.americanbar.org/natsecurity/patriotdebates/lone-wolf–2#rebuttal; Stand: 1.5.2012].

Spendel, Günter, Beweisverbote im Strafprozeß. NJW 1966, S. 1102–1108.

Stacy, Thomas, The Constitution in Conflict: Espionage Prosecutions, the Right to Present a Defense, and the State Secrets Privilege. U. Colo. L. Rev. (58) 1987, S. 177–254.

Stahl, Rudolf/Demuth, Ralf, Strafrechtliches Verwertungsverbot bei Verletzung des Steuergeheimnisses. Ein Zwischenruf im Fall Zumwinkel. DStR 2008, S. 600–604.

Standler, Ronald, Foreign Intelligence Surveillance Act: Unconstitutional or Bad Idea. 2007 [abrufbar unter: http://www.rbs0.com/FISA.pdf; Stand: 1.5.2012].

Stimson, Charles/Carafano, James, Treating Terrorism Solely as a Law Enforcement Matter – Not Miranda – Is the Problem. 2010 [abrufbar unter: http://thf_media.s3.amazonaws.com/2010/pdf/wm_2898.pdf; Stand: 1.5.2012].

Storbeck, Jürgen, Ansätze und Entwicklungsmöglichkeiten europäischer Intelligencestrukturen. In: Thomas Jäger/Anna Daun (Hrsg.), Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009, S. 155–167 [zit.: *Storbeck,* in: Jäger/Daun].

Strauß, Michael, Das Ende der Ermittlungsbefugnis der Staatsanwaltschaft. NStZ 2006, S. 556–560.

Stuckenberg, Carl-Friedrich, Das zähe Ringen um die Rechtsstellung der Gefangenen von Guantánamo Bay. JZ 2006, S. 1142–1151.

Systematischer Kommentar zur Strafprozeßordnung. Mit GVG und EMRK. Hrsg. von Jürgen Wolter. 4. Aufl. Köln 2010 (Bd. 2), 2011 (Bd. 3) [zit.: SK-StPO-*Bearbeiter*].

Swire, Peter, Privacy and Information Sharing in the War on Terrorism. Vill. L. Rev. (51) 2006, S. 951–980.

Tettinger, Peter/Erbguth, Wilfried/Mann, Thomas, Besonderes Verwaltungsrecht. 10. Aufl. Heidelberg 2009.

Thaman, Stephen, USA. In: Walter Perron (Hrsg.), Die Beweisaufnahme im Strafverfahrensrecht des Auslands. Rechtsvergleichendes Gutachten im Auftrag des Bundesministeriums der Justiz. Freiburg 1995, S. 489–547 [zit.: *Thaman,* in: Perron].

Thamm, Berndt, Ist das Trennungsgebot noch aktuell? In: Kai Hirschmann/Christian Leggemann (Hrsg.), Der Kampf gegen den Terrorismus. Strategien und Handlungserfordernisse in Deutschland. Berlin 2003, S. 235–254 [zit.: *Thamm,* in: Hirschmann/Leggemann].

Thompson, Alan/Nored, Lisa/Worrall, John/Hemmens, *Craig,* An Introduction to Criminal Evidence. A Casebook Approach. Oxford/New York 2008.

Tiedemann, Klaus/Sieber, Ulrich, Die Verwertung des Wissens von V-Leuten im Strafverfahren. Analyse und Konsequenzen der Entscheidung des Großen Senats des BGH. NJW 1984, S. 753–762.

Treverton, Gregory, Intelligence, Law Enforcement, and Homeland Security. 2002 [abrufbar unter: http://tcf.org/publications/pdfs/pb278/treverton-intelligence.pdf; Stand: 1.5.2012; zit.: *Treverton,* Intelligence].

– Reorganizing U.S. Domestic Intelligence. Assessing the Options. Santa Monica, California, 2008 [abrufbar unter: http://www.rand.org/pubs/monographs/MG767.html; Stand: 1.5.2012; zit.: *Treverton*, Reorganizing].

Trüg, Gerson, Lösungskonvergenzen trotz Systemdivergenzen im deutschen und US-amerikanischen Strafverfahren. Ein strukturanalytischer Vergleich am Beispiel der Wahrheitserforschung. Tübingen 2003.

Turner, Serrin/Schulhofer, Stephen, The Secrecy Problem in Terrorism Trials. 2005 [abrufbar unter http://www.brennancenter.org/sites/default/files/legacy/publications/20050000.TheSecrecyProbleminTerrorismTrials.pdf; Stand: 1.5.2012].

Vervaele, John, Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law? Utrecht L. Rev. (1) 2005, S. 1–27.

– The Anti-Terrorist Legislation in the US: Inter Arma Silent Leges? EJCCL & CJ (13) 2005, S. 201–254.

– Special Procedural Measures and Respect of Human Rights: General Report. RIDP/IRPL 2009, S. 75–123.

Villaverde, Mark, Structuring the Prosecutor's Duty to Search the Intelligence Community for Brady Material. Cornell L. Rev. (88) 2003, S. 1471–1548.

Vorbeck, Hans, Neue Aufgaben, neue Strukturen? Herausforderungen für Nachrichtendienste und Sicherheitsbehörden in Europa. In: Thomas Jäger/Anna Daun (Hrsg.), Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009, S. 293–302 [zit.: *Vorbeck,* in: Jäger/Daun].

Wabnitz, Heinz-Bernd/Janovsky, Thomas, Handbuch des Wirtschafts- und Steuerstrafrechts. 3. Aufl. München 2007 [zit.: Wabnitz/Janovsky-*Bearbeiter*].

Wache, Volkhard, Die Strafverfolgung islamistischer Terroristen. In: Kai Hirschmann/Christian Leggemann (Hrsg.), Der Kampf gegen den Terrorismus, Strategien und Handlungserfordernisse in Deutschland. Berlin 2003, S. 143–152 [zit.: *Wache,* in: Hirschmann/Leggemann].

Walker, Clive, Intelligence in Counter-Terrorism Processes. Washington DC 2010.

Walter, Gerhard, Freie Beweiswürdigung. Tübingen 1979.

Walter, Tonio, XVIIIth International Congress of Penal Law. RIDP/IRPL 2009, S. 161–178.

Wattenberg, Andreas, Die Rechtsprechung des Europäischen Gerichtshofs zum mittelbaren Zeugenbeweis – zugleich eine Anm. zum Urteil des BGH vom 11.2.2000 – 3 StR377/99. StV 2000, S. 688–696.

Waxman, Matthew/Barak-Erez, Daphne, Secret Evidence and the Due Process of Terrorist Detentions. Colum. J. Transnat'l L. (48:3) 2009, S. 3–64.

Weichert, Thilo, Informationelle Selbstbestimmung und strafrechtliche Ermittlung. Zum verfassungskonformen Technikeinsatz im Strafverfahren. Pfaffenweiler 1990.

Weigend, Thomas, Empfehlen sich gesetzliche Änderungen, um Zeugen und andere nicht beschuldigte Personen im Strafprozessrecht besser vor Nachteilen zu bewahren? Gutachten C für den 62. Deutschen Juristentag. In: Ständige Deputation des Deutschen Juristentages (Hrsg.), Gutachten [Teil A–E]. München 1998, C 1-C 131 [zit.: *Weigend,* in: DJT].

Weisser, Niclas-Frederic, Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) – Rechtsprobleme, Rechtsform und Rechtsgrundlagen. NVwZ 2011, S. 142–146.

Welp, Jürgen, Rechtsprechungsanmerkung zu BGH NStZ 1995, 601. NStZ 1995, S. 602–604.

– Die Strafgerichtsbarkeit des Bundes. NStZ 2002, S. 1–8.

Werthebach, Eckart/Droste-Lehnen, Bernadette, Organisierte Kriminalität. ZRP 1994, S. 57–65.

Weßlau, Edda, Vorfeldermittlungen. Probleme der Legalisierung „vorbeugender Verbrechensbekämpfung" aus strafprozeßrechtlicher Sicht. Berlin 1989.

Whitney, Justin, FISA's Future: An Analysis of Electronic Surveillance in Light of the Special Needs Exception to the Fourth Amendment 2007 [abrufbar unter: http://www.washburnlaw.edu/wlj/47–1/articles/whitney-justin.pdf; Stand: 1.5.2012].

Widmaier, Gunter, Münchener Anwaltshandbuch. Strafverteidigung. München 2006 [zit.: Widmaier-*Bearbeiter]*.

Wolff, Heinrich, Die Grenzverschiebung von polizeilicher und nachrichtendienstlicher Sicherheitsgewährleistung. DöV 2009, S. 597–606.

– Der nachrichtendienstliche Geheimnisschutz und die parlamentarische Kontrolle. JZ 2010, S. 173–180.

Wolff, Peter, Datenerhebung und -verarbeitung bei den Sicherheitsbehörden unter Berücksichtigung einer neuen Übermittlungskonzeption. Frankfurt a.M./New York 1997.

Wölfl, Bernd, Vorermittlungen der Staatsanwaltschaft. JuS 2001, S. 478–482.

Wollweber, Harald, Nochmals: Das Strafverfahrensänderungsgesetz 1999. NJW 2000, S. 3623–3625.

Wollweber, Tina, Die Zuständigkeit des Generalbundesanwalts in Staatsschutzsachen nach § 120 Abs. 1 und Abs. 2 GVG. Frankfurt a.M. 2010.

Wolter, Jürgen, Datenschutz und Strafprozeß. Zum Verhältnis von Polizeirecht und Strafprozessrecht. ZStW 107 (1995), S. 793–842.

Wolter, Jürgen, Formen der Vorermittlungsverfahren und Reform des Ermittlungsverfahrens. Zugleich: Grundlagen der Alternativentwürfe AE-ZVR und AE-EV. In: Arthur Kreuzer/Herbert Jäger/Harro Otto/Stephan Quensel/Klaus Rolinski (Hrsg.), Fühlende und denkende Kriminalwissenschaften. Ehrengabe für Anne-Eva Brauneck. Mönchengladbach 1999, S. 501–532.

Woods, J., Lone Wolf – Targeting the Loosely-Affiliated Terrorist 2005 [abrufbar unter: http://apps.americanbar.org/natsecurity/patriotdebates/lone-wolf–2#rebuttal; Stand: 1.5. 2012].

Würtenberger, Thomas/Heckmann, Dirk, Polizeirecht in Baden-Württemberg. 6. Aufl. Heidelberg 2005.

Yaroshefsky, Ellen, Secret Evidence is Slowly Eroding the Adversary System: CIPA and FISA in the Courts. Hofstra L. Rev. (34) 2006, S. 1063–1092.

Young, Mark, What Big Eyes and Ears you Have! A New Regime for Covert Governmental Surveillance. Fordham L. Rev. (34) 2001, S. 1017–1109.

Zabel, Richard/Benjamin, James, In Pursuit of Justice. Prosecuting Terrorism Cases in the Federal Courts. New York 2008.

Zacharias, Klaus, Der gefährdete Zeuge im Strafverfahren. Berlin 1997.

Ziercke, Jörg, Terrorismusbekämpfung – Die Zusammenarbeit der Sicherheitsbehörden in Deutschland aus Sicht der Polizei. In: Bundesamt für Verfassungsschutz (Hrsg.), Terrorismusbekämpfung in Europa – Herausforderung für die Nachrichtendienste – Symposium, Vorträge auf dem 7. Symposium des Bundesamtes für Verfassungsschutz am 8. Dezember 2008. Köln 2008, S. 40–50 [zit.: *Ziercke,* in: Bundesamt für Verfassungsschutz].

Zöller, Mark, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten. Zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz. Heidelberg 2002 [zit.: *Zöller,* Informationssysteme].

– Datenübermittlungen zwischen Polizei, Strafverfolgungsbehörden und Nachrichtendiensten. In: Fredrik Roggan/Martin Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit. Berlin 2006, S. 447–509 [zit.: *Zöller,* in: Roggan/Kutscha].

– Der Rechtsrahmen der Nachrichtendienste bei der „Bekämpfung" des internationalen Terrorismus. JZ 2007, S. 763–771.

– Heimlichkeit als System. StraFo 2008, S. 15–22.

– Terrorismusstrafrecht. Ein Handbuch. Heidelberg/Hamburg 2009 [zit.: *Zöller,* Terrorismusstrafrecht].

Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht

Die zentralen Veröffentlichungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht werden in Zusammenarbeit mit dem Verlag Duncker & Humblot in den folgenden vier Unterreihen der „Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht“ vertrieben:

- „Strafrechtliche Forschungsberichte“,
- „Kriminologische Forschungsberichte“,
- „Interdisziplinäre Forschungen aus Strafrecht und Kriminologie“ sowie
- „Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung“.

Diese Publikationen können direkt über das Max-Planck-Institut unter <www.mpicc.de> oder über den Verlag Duncker & Humblot unter <www.duncker-humblot.de> erworben werden.

Darüber hinaus erscheinen im Hausverlag des Max-Planck-Instituts in der Unterreihe „research in brief“ zusammenfassende Kurzbeschreibungen von Forschungsergebnissen und in der Unterreihe „Arbeitsberichte“ Veröffentlichungen vorläufiger Forschungsergebnisse. Diese Veröffentlichungen können über das Max-Planck-Institut bezogen werden.

Detaillierte Informationen zu den einzelnen Publikationen des Max-Planck-Instituts für ausländisches und internationales Strafrecht sind unter <www.mpicc.de> abrufbar.

The main research activities of the Max Planck Institute for Foreign and International Criminal Law are published in the following four subseries of the “Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht” (Research Series of the Max Planck Institute for Foreign and International Criminal Law), which are distributed in cooperation with the publisher Duncker & Humblot:

- “Strafrechtliche Forschungsberichte” (Reports on Research in Criminal Law),
- “Kriminologische Forschungsberichte” (Reports on Research in Criminology),
- “Interdisziplinäre Forschungen aus Strafrecht und Kriminologie” (Reports on Interdisciplinary Research in Criminal Law and Criminology), and
- “Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung” (Collection of Foreign Criminal Laws in German Translation).

These publications can be ordered from the Max Planck Institute at <www.mpicc.de> or from Duncker & Humblot at <www.duncker-humblot.de>.

Two additional subseries are published directly by the Max Planck Institute for Foreign and International Criminal Law: “research in brief” contains short reports on results of research activities, and “Arbeitsberichte” (working materials) present preliminary results of research projects. These publications are available at the Max Planck Institute.

Detailed information on all publications of the Max Planck Institute for Foreign and International Criminal Law can be found at <www.mpicc.de>.

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aus dem strafrechtlichen Veröffentlichungsprogramm:

S 144 *Michael Albrecht*
Die Kriminalisierung von Dual-Use-Software
2014 • 297 Seiten • ISBN 978-3-86113-812-9 € 40,00

S 143 *Zunyou Zhou*
Balancing Security and Liberty
Counter-Terrorism Legislation in Germany and China
2014 • 352 Seiten • ISBN 978-3-86113-813-6 € 40,00

S 142 *Nadine Dombrowski*
Extraterritoriale Rechtsanwendung im Internet
2014 • 206 Seiten • ISBN 978-3-86113-814-3 € 31,00

S 141 *Gang Wang*
Die strafrechtliche Rechtfertigung von Rettungsfolter
Ein Rechtsvergleich zwischen Deutschland und den USA
2014 • 428 Seiten • ISBN 978-3-86113-815-0 € 41,00

S 140 *Ulrich Sieber / Marc Engelhart*
Compliance Programs for the Prevention of Economic Crimes
An Empirical Survey of German Companies
2014 • 312 Seiten • ISBN 978-3-86113-816-7 € 40,00

S 139 *Susanne Rheinbay*
Die Errichtung einer Europäischen Staatsanwaltschaft
2014 • 347 Seiten • ISBN 978-3-86113-819-8 € 35,00

S 138 *Sarah Herbert*
Grenzen des Strafrechts bei der Terrorismusgesetzgebung
Ein Rechtsvergleich zwischen Deutschland und England
2014 • 300 Seiten • ISBN 978-3-86113-820-4 € 35,00

S 137 *Nadine Zurkinden*
Joint Investigation Teams
Chancen und Grenzen von gemeinsamen Ermittlungsgruppen
in der Schweiz, Europa und den USA
2013 • 396 Seiten • ISBN 978-3-86113-821-1 € 41,00

S 136 *Nico Herbert*
Strafrechtlicher Schutz von EU-Subventionen
Reichweite und Grenzen in Deutschland, Österreich und England
am Beispiel nicht wirtschaftsfördernder Subventionen
2013 • 320 Seiten • ISBN 978-3-86113-823-5 € 38,00

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aktueller Publikationen aus dem kriminologischen Veröffentlichungsprogramm:

K 166 *Ramin Tehrani*
Die „Smart Sanctions" im Kampf gegen den Terrorismus und als Vorbild einer präventiven Vermögensabschöpfung
Berlin 2014 • 256 Seiten • ISBN 978-3-86113-247-9 € 35,00

K 165 *Daniela Cernko*
Die Umsetzung der CPT-Empfehlungen im deutschen Strafvollzug
Eine Untersuchung über den Einfluss des Europäischen Komitees zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe auf die deutsche Strafvollzugsverwaltung
Berlin 2014 • 455 Seiten • ISBN 978-3-86113-246-2 € 39,00

K 164 *Franziska Kunz*
Kriminalität älterer Menschen
Beschreibung und Erklärung auf der Basis von Selbstberichtsdaten
Berlin 2014 • 387 Seiten • ISBN 978-3-86113-244-8 € 35,00

K 163 *David Jensen*
Maras
A study of their origin, international impact, and the measures taken to fight them
Berlin 2013 • 245 Seiten • ISBN 978-3-86113-243-1 € 35,00

K 161 *Gunda Wößner, Roland Hefendehl, Hans-Jörg Albrecht* (Hrsg.)
Sexuelle Gewalt und Sozialtherapie
Bisherige Daten und Analysen zur Längsschnittstudie „Sexualstraftäter in den sozialtherapeutischen Abteilungen des Freistaates Sachsen"
Berlin 2013 • 274 Seiten • ISBN 978-3-86113-241-7 € 35,00

K 159 *Andreas Armborst*
Jihadi Violence
A study of al-Qaeda's media
Berlin 2013 • 266 Seiten • ISBN 978-3-86113-119-9 € 35,00

K 158 *Martin Brandenstein*
Auswirkungen von Hafterfahrungen auf Selbstbild und Identität rechtsextremer jugendlicher Gewalttäter
Berlin 2012 • 335 Seiten • ISBN 978-3-86113-118-2 € 35,00

K 157 *Ghassem Ghassemi*
Criminal Policy in Iran Following the Revolution of 1979
A Comparative Analysis of Criminal Punishment and Sentencing in Iran and Germany
Berlin 2013 • 265 Seiten • ISBN 978-3-86113-116-8 € 35,00

K 156 *Gunther Olt*
Pressefreiheit im Kontext strafrechtlicher Ermittlungsmaßnahmen
Berlin 2013 • 265 Seiten • ISBN 978-3-86113-114-4 € 35,00