Beiträge zum Strafrecht –
Contributions to Criminal Law 11

Nico Gallus

Smart Speaker im Lichte der StPO

Möglichkeiten des Zugriffs und Problematiken der Verwertbarkeit

Nomos

Beiträge zum Strafrecht –
Contributions to Criminal Law

herausgegeben von

Prof. Dr. Jochen Bung, Universität Hamburg

Prof. Dr. Christoph Burchard,
Goethe-Universität Frankfurt

Prof. Dr. Jörg Eisele, Universität Tübingen

Prof. Dr. Elisa Hoven, Universität Leipzig

Prof. Dr. Johannes Kaspar, Universität Augsburg

Prof. Dr. Tobias Reinbacher,
Julius-Maximilians-Universität Würzburg

Prof. Dr. Dr. Frauke Rostalski, Universität zu Köln

Band 11

Nico Gallus

Smart Speaker im Lichte der StPO

Möglichkeiten des Zugriffs und Problematiken der Verwertbarkeit

Nomos

The book processing charge was funded by the Baden-Württemberg Ministry of Science, Research and Arts in the funding programme Open Access Publishing and the University of Freiburg

Dekan:	Prof. Dr. Katharina von Koppenfels-Spies
Erstgutachter:	Prof. Dr. Gerson Trüg
Zweitgutachter:	Prof. Dr. Dr. h.c. Walter Perron
Tag der mündlichen Prüfung:	10. November 2021
Dissertationsort:	Albert-Ludwigs-Universität Freiburg im Breisgau
Erscheinungsjahr:	2022

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

1. Auflage 2022

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-8487-8534-6
ISBN (ePDF): 978-3-7489-2895-9

DOI: https://doi.org/10.5771/9783748928959

Onlineversion
Nomos eLibrary

Meinen Eltern

Vorwort

Die vorliegende Arbeit entstand im Zeitraum von Juli 2019 bis Oktober 2020 und wurde im Wintersemester 2021/2022 vom Fachbereich Rechtswissenschaft der Albert-Ludwigs-Universität Freiburg als Dissertation angenommen. Zeitlich nachfolgend veröffentlichte Literatur sowie ergangene Rechtsprechung konnte ohne Anspruch auf Vollständigkeit noch bis Oktober 2021 berücksichtigt werden. Auf § 95a StPO n.F. wurde nicht mehr gesondert eingegangen.

Mein besonderer Dank gilt zuvorderst meinem Doktorvater, *Herrn Professor Dr. Gerson Trüg*. Seine stetige Unterstützung sowie konstruktiven Anmerkungen und Hinweise haben wesentlich zum Gelingen der Arbeit beigetragen. Zudem hat er mir stets die wissenschaftliche Freiheit gelassen, eine eigenständige Position zu entwickeln und zu vertreten. Bedanken möchte ich mich zudem bei *Herrn Professor Dr. Dr. h.c. Walter Perron* für die zügige Erstellung des Zweitgutachtens mitsamt den hierin enthaltenen wertvollen Anmerkungen und Denkanstößen.

Mein herzlicher Dank gilt außerdem dem *Konsortium Baden-Württemberg* für die Finanzierung des Drucks und der Veröffentlichung als Open-Access-Publikation.

Weiterhin möchte ich mich bei meinen Wegbegleitern aus Freiburger Studienzeiten bedanken. Die gemeinsam erlebte Zeit wird mir immer in positiver Erinnerung bleiben. Insbesondere die zahlreichen gemeinsamen Mittags- und Nachmittagspausen haben mir das gesamte Studium sowie die Anfertigung dieser Arbeit wesentlich erleichtert. Namentlich erwähnen will ich dabei ganz besonders *Lisa Ahlers*, *Claudio Aliprandi*, *Axel Garrels*, *Dr. Raphael Hilser*, *Merle Hörr*, *Sebastian Langer*, *Sarah Leikam*, *Lars Mager*, *Nebiyu Mahmud*, *Paul Strohmaier*, *Sandra Utz*, *Raphael Wagner* sowie *Dr. Lukas Zeyher*. *Dr. Raphael Hilser* danke ich in diesem Zusammenhang insbesondere für seine Zeit und Mühen, den Erstentwurf meiner Dissertation kritisch zu lesen und umfassend zu prüfen. Für ihre abschließende Durchsicht der Arbeit danke ich zudem meiner Mutter *Elke Gallus*.

Bedanken möchte ich mich auch bei meiner Großtante *Gisela Dietze* für ihre finanzielle Unterstützung während meines Studiums.

Ein ganz besonderer Dank gilt meiner Familie. Auf den Rückhalt meiner Eltern *Elke* und *Karl Gallus*, meines Bruders *Luca Gallus* sowie meiner Großeltern *Waltraud* und *Arnold Hoferer* und *Anni Wutke* konnte und kann

ich mich jederzeit verlassen. Meinen Eltern *Elke* und *Karl Gallus* gebührt schließlich mein allergrößter Dank. Ihr unerschütterliches Vertrauen in mich, ihr Zuspruch sowie ihre stetige in jeder Hinsicht uneingeschränkte und bedingungslose Unterstützung sowie Förderung haben mir meine juristische Ausbildung erst ermöglicht.

Nordrach, im November 2021 *Nico Gallus*

Inhaltsverzeichnis

Abkürzungsverzeichnis 19

§ 1 Einführung 23

§ 2 Technischer Hintergrund 29

A. Funktionsweise Smart Speaker 30

B. Cloud Computing 34

I) Definitionsansätze 35

II) Ebenenstruktur 38

1) IaaS Cloud-Computing 38

2) PaaS Cloud-Computing 39

3) SaaS Cloud-Computing 40

4) FaaS-Cloud Computing 41

III) Einordnung eines Sprachassistenten in Form eines Smart Speakers 42

IV) Erscheinungsformen Cloud-Computing 43

C. Nutzen und Risiken 44

§ 3 Elektronische Daten im Strafverfahren 48

A. Ziel des Strafverfahrens 48

I) Allgemeines 48

II) Beschränkungen 50

1) Vorbehalt des Gesetzes 50

2) Verfahrensrechtliche Beschränkungen 52

a) Verdachtsgrad 52

b) Straftatenkataloge 52

c) Subsidiaritätsklauseln 53

d) Richtervorbehalt 53

3) Beweisverwertungsverbote 54

a) Wahrung der Rechte des Einzelnen 55

b) Schutz der Wahrheitsfindung 56

c) Aufrechterhaltung der hoheitlichen Straflegitimation 57

d) Disziplinierungsgedanke 58
B. Elektronische Daten im Strafprozess 60
I) Einbringung elektronischer Daten in den Strafprozess 61
1. Zeugenbeweis 62
2. Sachverständigenbeweis 63
3. Urkundenbeweis 63
4. Inaugenscheinnahme 65
II) Einordnung der Audioaufzeichnungen eines Sprachassistenten 65
III) Beweiswert 68
IV) Vor- und Nachteile digitaler Daten als Beweismittel 71

§ 4 Zugriffsmöglichkeiten zur Gewinnung elektronischer Daten 73

A. Allgemeines 73
I) Grundsatz 73
II) Datenarten 74
1) Bestandsdaten 74
2) Verkehrsdaten 74
3) Inhaltsdaten 75
4) Zusammenfassung 75
B. Ermächtigungsgrundlagen 77
I) § 100a StPO 77
1) Tatbestandsmerkmal der Kommunikation 77
a) Weiter technischer Telekommunikationsbegriff 77
aa) Technische Auslegung 78
bb) Technikorientierte Auslegung 78
b) Grundrechtsanaloger Telekommunikationsbegriff 79
c) Enger strafverfahrensrechtlicher Telekommunikationsbegriff 80
2) Nutzung eines Smart Speakers als Kommunikation i.S.d. § 100a Abs. 1 S. 1 StPO 81
a) Vor der Übertragung 82
b) Während des Übertragungsweges 82
aa) Rein technische Auslegung 83
bb) Technikorientierter Telekommunikationsbegriff 83
cc) Grundrechtsanaloger Telekommunikationsbegriff 84
(1) Grundsätzliches 84

(2) Sinn und Zweck der Grundrechte 86
(3) Massen- oder Individualkommunikation 86
(4) Teilnehmer an einem Kommunikationsvorgang 88
(4.1) Entwicklung der Rechtsprechung 88
(4.1.1) Auslesen eines Endgerätespeichers 89
(4.1.2) IMSI-Catcher Beschluss 90
(4.1.3) Surfen im Internet-Beschluss 92
(4.1.4) Zwischenergebnis 95
(4.2) Ansichten in der Literatur 95
(4.2.1) Multipersonale Strömung 95
(4.2.2) Differenzierende Ansicht 96
(4.2.3) Unipersonale Strömung 96
(4.3) Stellungnahme 97
(5) Zwischenergebnis 101
dd) Strafprozessualer Telekommunikationsbegriff 101
c) Auf der Cloud des Diensteanbieters 102
aa) Technischer Kommunikationsbegriff 102
bb) Technikorientierter Telekommunikationsbegriff 102
cc) Grundrechtsanaloger Telekommunikationsbegriff 103
dd) Strafprozessualer Telekommunikationsbegriff 106
d) Zwischenergebnis 106
e) Stellungnahme 107
aa) Kritik an den technischen Auffassungen 107
bb) Kritik an der grundrechtsanalogen Auffassung 110
cc) Lösung 113
3) Eigener Vorschlag eines strafprozessualen Telekommunikationsbegriffes 114
a) Erforderliche Personenanzahl 114
aa) Auslegung nach Wortsinn 114
bb) Historische Auslegung 115
cc) Systematische Auslegung 115
dd) Teleologische Auslegung 116
b) Telekommunikationswille 118
c) Zwischenergebnis 120

d) Nutzung eines Sprachassistenten in der Form eines Smart Speakers im Sinne des personell-individuellen Telekommunikationsbegriffs 121
4) Verschlüsselung der Daten 122
II) § 100a Abs. 1 S. 2 StPO n.F. 122
1) Allgemeines 122
2) Verfassungsmäßigkeit des § 100a Abs. 1 S. 2 StPO n.F. 123
3) Informationstechnisches System 128
a) Allgemeines 128
b) Doppelnatur 129
aa) Begriffsverständnis im Sinne des § 100a Abs. 1 S. 2, 3 StPO 130
bb) Server des Dienstleistungsanbieters als informationstechnisches System 130
4) Ergebnis 131
III) § 100a Abs. 1 S. 3 StPO n.F. 132
1) Allgemeines 132
2) Verfassungsmäßigkeit der Vorschrift 133
a) Keine Begrenzung auf laufende Telekommunikation 133
b) Verstoß gegen die Maßstäbe des IT-Grundrechts 135
c) Verhältnismäßigkeit hinsichtlich des Straftatenkatalog 136
d) Erhöhte Eingriffsintensität 137
e) Zwischenergebnis 140
IV) Überwachung eines Sprachassistenten als Minusmaßnahme zu § 100a StPO 140
V) § 100b StPO 141
1) Infiltration des Endgeräts 142
a) Möglichkeiten der Infiltration 142
b) Infiltration des Endgeräts zur Online-Durchsuchung 144
c) Infiltration des Endgeräts zur Online-Live-Überwachung 144
2) Zugriff auf Mikrofon und Kamera 145
a) Wortlaut 145
b) Historie 146
c) Systematik 147
d) Telos 149
e) Zwischenergebnis 149

3) Infiltration der Server des Dienstleistungsanbieters 150
4) Verfassungswidrigkeit des § 100b StPO 151
a) Fehlende ultima-ratio Ausgestaltung 151
b) Unzureichende Ausgestaltung des Kernbereichsschutzes 153
c) Zu weiter Anlasstatenkatalog 155
d) Fehlerhafter Schutz von Berufsgeheimnisträgern 156
e) Zwischenergebnis 158
5) Ergebnis 158
VI) § 100c StPO 159
1) Smart Speaker als technisches Mittel im Sinne des § 100c StPO 160
a) Wortlaut 160
b) Historie 161
c) Systematik 161
d) Telos 163
2) Kollision mit IT-Grundrecht 163
3) Stellungnahme 165
4) Verpflichtung der Hersteller zur Mitwirkung 169
VII) Kombination aus § 100b und § 100c StPO 170
VIII) § 100f StPO 171
IX) §§ 102 ff., 110 Abs. 3 StPO 171
1) Physische Hardware 172
2) Digitale Serverdaten 173
a) Entwicklung des § 110 Abs. 3 StPO 173
b) Voraussetzungen 174
aa) Allgemeines 174
bb) Möglichkeiten der Sichtung 176
cc) Möglichkeiten zur Passworterlangung 178
(1) Technische Entschlüsselung 179
(2) Bestandsdatenabfrage gem. § 100j StPO 180
(3) Auskunftsverlangen gem. §§ 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG 184
(4) Zwischenergebnis 186
3) § 110 Abs. 3 StPO im Verhältnis zum Dienstleistungsanbieter 187

X) § 94 ff. StPO 188
1) Durchsuchung und Beschlagnahme beim Verdächtigen 188
a) Ermächtigungsgrundlage zur Beschlagnahme 190
aa) § 99 StPO 190
bb) § 94 StPO 191
2) Durchsuchung und Beschlagnahme beim Dienstleistungsanbieter 195
3) Ergebnis 198
XI) Ermittlungsgeneralklausel, § 161 StPO 199
XII) Übergeordnete Problematik: Serverstandort 201
XII) Ergebnis 202

§ 5 Verwertbarkeit 204

A. Beweiserhebungsverbote 204
I) Beweisthemaverbot 205
1) Der Kernbereichsschutz auf Erhebungsebene 207
a) Entwicklung des Kernbereichsschutzes 207
b) Verfassungsrechtliche Grundlage 208
c) Negative Kernbereichsprognose 209
aa) Indikatoren der negativen Kernbereichsprognose 210
(1) Räumliche Situation 210
(2) Vertrauensverhältnis der Kommunizierenden 211
(3) Anzahl der Kommunizierenden 214
(4) Thematik 215
bb) Verhältnis der Indikatoren 216
d) Einschränkungen des Kernbereichs 218
aa) Art des Gesprächs 218
bb) Inhalt: Straftatvorbehalt 220
(1) Im Rahmen der Tagebuchaufzeichnung 220
(1.1) Tagebuchentscheidungen des BGH 1964 und 1988 220
(1.2) Erste Tagebuchentscheidung des BVerfG vom 14.09.1989 – 2 BvR 1062/87 221

(2) Im Rahmen eines Zwiegesprächs 223
(2.1) Urteil zum Großen Lauschangriff des BVerfG vom 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99 223
(2.2) Zweite Tagebuchentscheidung des BVerfG vom 26.06.2008 – 2 BvR 219/08 223
(2.3) Neuere Rechtsprechung des BVerfG 224
(2.4) Auffassung Roxins 226
(3) Im Rahmen eines Selbstgespräches 227
(3.1) Die BGH-Rechtsprechung 227
(3.2) Kritik 229
(3.3) Einschränkung auf beichtende Selbstgespräche 230
2) Stellungnahme 231
a) Allgemeines 231
b) Der Sozialbezug 234
c) Umgang mit einem Selbstgespräch 235
d) Umgang mit einem Zwiegespräch 238
e) Zusammenfassung 239
3) Umgang mit Mischgesprächen 240
a) Weites Verständnis 241
b) Enges Verständnis 242
c) Stellungnahme 242
4) Nachgelagerter Kernbereichsschutz 244
a) Umfang nachgelagerter Kontrollen 245
b) Zusammenspiel der praktischen Möglichkeiten zum Schutz des Kernbereichs 247
c) Stellungnahme 249
5) Der Kernbereichsschutz bei übrigen Maßnahmen 250
6) Übertragung der Maßstäbe auf die Nutzung eines Smart Speaker zur Strafverfolgung 251
a) Überwachung mündlicher Informationsabfragen während aktiver Nutzung des Smart Speaker 252
b) Einsatz eines Sprachassistenten als Wanze 256
II) Beweismittelverbote und Beweismethodenverbote 256

B. Beweisverwertungsverbote 257
I) Unselbstständige Beweisverwertungsverbote 258
1) Geschriebene Beweisverwertungsverbote 258

2) Der Kernbereich als Auslöser eines absoluten Verwertungsverbot 259
a) Der Sozialbezug 259
b) Geheimhaltungswille 260
3) Ungeschriebene Beweisverwertungsverbote 261
a) Rechtskreistheorie 262
b) Schutzzwecktheorie 264
c) Abwägungslehre 265
e) Stellungnahme 267
aa) Problematik der Abwägungslehre 267
bb) Ansatz Rehbeins 269
cc) Kriteriengewichtung im Rahmen der Abwägungslösung 270
dd) Lösung 271
4) Konsequenzen für mögliche Konstellationen beim Zugriff auf einen Sprachassistenten 276
a) Fehlende richterliche Anordnung 276
b) Fehlende Ermächtigungsgrundlage 280
c) Falsche Ermächtigungsgrundlage 280
aa) §§ 102, 103 StPO 281
bb) § 100a StPO 282
II) Selbstständige Beweisverwertungsverbote 283
1) Grundrechtsbeeinträchtigungen beim Zugriff auf Sprachassistenten 284
a) Art. 13 GG 284
aa) Schutzbereich Art. 13 GG 284
(1) Weite Auslegung 285
(2) Enge Auslegung 286
(3) Vermittelnde Ansichten 286
(4) Stellungnahme 287
bb) Beeinträchtigung 288
(1) Im Rahmen einer Wohnraumüberwachung nach § 100c StPO 288
(2) Im Rahmen eines Zugriffs über § 100b StPO 289
(3) Im Rahmen einer Maßnahme nach § 110 Abs. 3 StPO 291
b) Art. 10 GG 292

c) Computergrundrecht 292
aa) Im Rahmen einer Wohnraumüberwachung nach § 100c StPO 293
bb) Im Rahmen eines Zugriffs über § 100b StPO 293
cc) Im Rahmen einer Maßnahme nach § 110 Abs. 3 StPO 296
d) Das Grundrecht auf informationelle Selbstbestimmung 296
2) Die Drei-Sphären-Theorie 298
3) Zwischenergebnis 300
4) Sonderkonstellation: Beweiserlangung durch Private 302
a) Beschlagnahme aufgrund eines Anfangsverdachts 303
b) Übermittlung einer autorisierten Aufzeichnung durch Dienstleistungsanbieter an die Strafverfolgungsbehörden 303
aa) § 201 Abs. 1 Nr. 1 StGB 305
bb) § 206 StGB 306
c) Übermittlung einer nicht autorisierten Aufzeichnung an die Strafverfolgungsbehörden 307
aa) § 201 Abs. 1 Nr. 1 StGB 307
bb) Voraussetzungen und Folgen einer rechtswidrigen Beweisgewinnung durch Private 309
(1) Lösung der Rechtsprechung und Teilen der Literatur 311
(2) Literaturstimmen 312
cc) Strafbarkeit gem. § 201 Abs. 2 Nr. 1 StGB 314
dd) Stellungnahme 316
d) Übermittlung etwaiger Hintergrundäußerungen Dritter während autorisierter Aufzeichnung 321
e) Exkurs: Richterliche Strafbarkeit durch Verwertung nach § 201 Abs. 1 Nr. 2 StGB 322
III) Zwischenergebnis 325
IV) Die Disponibilität eines Beweisverwertungsverbotes 326
1) Verwertbarkeit des Beweismittels zur eigenen Entlastung 326
2) Teilweise Verwertbarkeit des Beweismittels zur eigenen Entlastung 331
a) ablehnende Position 332
b) Mühlenteichtheorie 332

c) Stellungnahme 333
3) Disponibilität eines Beweismittels bei mehreren Mitangeklagten 334
a) Reichweite eines Beweisverwertungsverbotes 334
b) Disponibilität zugunsten der Verwertbarkeit 336
aa) Eingriff in die Rechtssphäre nur eines Angeklagten 336
bb) Eingriff in die Rechtsphäre sämtlicher Mitangeklagter 338
cc) Problematik einer gesplitteten Tatsachenfeststellung 339
4) Zwischenergebnis 340
V) Fernwirkung 341
1) Kernbereichsbetroffenheit 342
2) Sonstige Fälle 343
a) Ablehnende Position 343
b) Befürwortende Position 344
c) Differenzierte Lösung 345
3) Stellungnahme 346
4) Geltendmachung von Löschungsansprüchen 349
C. Nutzung der Daten zur Gefahrenabwehr 350
I) Umwidmung repressiv erhobener Daten zu präventiven Zwecken 350
II) Möglichkeiten der praktischen Umsetzung 356
D. Ergebnis 357

§ 6 Ausblick und Zusammenfassung 360

Literaturverzeichnis 363

Abkürzungsverzeichnis

a.A./a.A.	anderer Ansicht/andere Auffassung
a.a.O.	Am angegebenen Ort
a.F.	Alte Fassung
Abs.	Absatz
AG	Aktiengesellschaft
Anm.	Anmerkung
AnwBl	Anwaltsblatt
AöR	Archiv des öffentlichen Rechts
Art.	Artikel
Az.	Aktenzeichen
BayObLG	Bayrisches Oberstes Landesgericht
BayVBl	Bayerische Verwaltungsblätter
BB	Betriebs-Berater
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Online-Kommentar
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BPolG	Bundespolizeigesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bspw.	Beispielsweise
BT	Besonderer Teil
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfGK	Kammerentscheidungen des Bundesverfassungsgerichts
BVwerG	Bundesverwaltungsgericht
Bzw.	Beziehungsweise
c´t	Magazin für Computertechnik

CB	Compliance Berater
ComputerR-HdB	Computerrechtshandbuch
CR	Computer und Recht
DAR	Deutsches Autorrecht
Ders.	Derselbe
Dies.	Dieselbe
DJT	Deutscher Juristentag
DÖV	Die öffentliche Verwaltung
DRiZ	Deutsche Richterzeitung
DSGVO	Datenschutz-Grundverordnung
DSRITB	DSRI-Tagungsband
Dt.	Deutscher
DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
Ebd.	Ebenda
EGMR	Europäischer Gerichtshof für Menschenrechte
Einl.	Einleitung
EMRK	Europäische Menschenrechtskonvention
f.	Folgende
FaaS	Function as a Service
FAZ	Frankfurter Allgemeine Zeitung
ff.	folgende
Fn.	Fußnote
FS	Festschrift
GA	Goltdammer´s Archiv für Strafrecht
GG	Grundgesetz
GK	Grundkurs
Grds.	Grundsätzlich
GS	Gedächtnisschrift
GVG	Gerichtsverfassungsgesetz
HH-Ko	Hamburger Kommentar
HK-GS	Handkommentar Gesamtes Strafrecht
HRRS	Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht
Hrsg.	Herausgeber
i.d.R.	In der Regel

i.S.d.	Im Sinne des
i.V.m.	In Verbindung mit
IaaS	Infrastructure as a Service
ITRB	IT-Rechts-Berater
JA	Juristische Arbeitsblätter
JR	Juristische Rundschau
JURA	Juristische Ausbildung
jurisPR-ITR	juris PraxisKommentar Internetrecht
JuS	Juristische Schulung
JZ	Juristenzeitung
K&R	Kommunikation & Recht
KJ	Kritische Justiz
KK	Karlsruher Kommentar
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LG	Landgericht
LR-StPO	Löwe-Rosenberg Großkommentar Strafprozessordnung
m.w.N.	mit weiteren Nachweisen
MDR	Monatsschrift für Deutsches Recht
MedienR	Medienrecht
MMR	Multimedia und Recht
MüKo	Münchener Kommentar
n.F.	Neue Fassung
NdsVbl	Niedersächsische Verwaltungsblätter
NJ	Neue Justiz
NJW	Neue Juristische Wochenschrift
NK	Nomoskommentar
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZV	Neue Zeitschrift für Verkehrsrecht
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht
OLG	Oberlandesgericht
PaaS	Platform as a Service
PinG	Privacy in Germany

PolR	Polizeirecht
Rn.	Randnummer
S.	Seite / Satz
SaaS	Software as a Service
Sog.	sogenannte/r
St. Rspr.	Ständige Rechtsprechung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StraFo	Strafverteidiger Forum
StrafR	Strafrecht
StRR	Strafrechtsreport
StudZR	Studentische Zeitschrift für Rechtswissenschaft
StV	Strafverteidiger
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
Urt	Urteil
Urt.	Urteil
v.	Vom
Var.	Variante
VBlBW	Verwaltungsblätter für Baden-Württemberg
Vgl.	Vergleiche
Vor.	Vorbemerkung
VwGO	Verwaltungsgerichtsordnung
WiJ	Journal der Wirtschaftsstrafrechtlichen Vereinigung e.V
Wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
z.B.	Zum Beispiel
ZD	Zeitschrift für Datenschutz
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
Zit.	Zitiert
ZJS	Zeitschrift für das Juristische Studium
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber- und Medienrecht
ZWH	Zeitschrift für Wirtschaftsstrafrecht und Haftung im Unternehmen

§ 1 Einführung

Noch Anfang des Jahrtausends waren sprachgesteuerte Technologien lediglich ein aus Filmen bekanntes Phänomen: Das Interagieren mit einem technischen Gerät ausschließlich mittels der eigenen Stimme, ließ allenfalls an den Alltag in einigen Jahrzehnten denken. Doch bereits seit Beginn der 2010er Jahre verbreiten sich sprachgesteuerten Geräte enorm. Es war damals kaum abzusehen, dass bis in das Jahr 2020 weltweit über 1,6 Milliarden Menschen zu den Nutzern digitaler Assistenten zählen würden.[1] Das gesamte „Internet of Things"[2] befindet sich in einem anhaltenden Wachstumsprozess und erlebt eine rasante Verbreitung, die dazu führt, dass bis heute etwa 50 Milliarden Geräte mit dem Internet verbunden sind; das sind durchschnittlich sieben Geräte pro Mensch.[3] Es wird erwartet, dass weltweit 200 Millionen Smart Speaker[4] bis 2023 verkauft werden.[5] Die Nutzung sog. Smart-Speaker erfreut sich nicht nur in deren Entwicklungsland den Vereinigten Staaten großer Beliebtheit, sondern auch in gesamt Europa. In Deutschland begann die Nutzung der Smart-Speaker mit der Einführung des Amazon Echo-Gerätes im Oktober 2016.[6] Seither erlebt die technische Neuheit national wie global einen stetigen Nutzungsanstieg.[7] Nach einer repräsentativen Umfrage von Mai 2020 im Auftrag des Digitalverbandes Bitkom nutzen mittlerweile zwei von fünf Internetnutzern (39 %) zumindest teilweise einen digitalen Assistenten. Über zwei Drittel der Nutzer eines Sprachassistenten geben

---

1 Statista-Dossier zu digitalen Sprachassistenten, S. 8, https://de.statista.com/statistik/studie/id/48227/dokument/digitale-sprachassistenten/ (zuletzt abgerufen am 31.10.2021).

2 Vgl. hierzu *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 3, Rn. 431 f.

3 *Czychowski/Siesmayer* in: Taeger/Pohle, ComputerR-HdB, Kap. 20.5, Rn. 4; *Ametsbichler*, DSRITB 2019, 497.

4 Vgl. zur genaueren Definition § 2. Der feststehende Begriff „Smart Speaker" umfasst nach dem hier zugrunde liegenden Verständnis ebenso den entsprechenden Plural.

5 Statista-Dossier zu digitalen Sprachassistenten, S. 5, https://de.statista.com/statistik/studie/id/48227/dokument/digitale-sprachassistenten/ (zuletzt abgerufen am 31.10.2021).

6 https://de.wikipedia.org/wiki/Amazon_Echo (zuletzt abgerufen am 31.10.2021).

7 *Miftari/Henrichs*, Zwischen innovativer Polizeiarbeit und neuem Managements, 297, 299.

darüber häufig oder sehr häufig Sprachbefehle ein.[8] Beinahe 40 % der Nutzer der Sprachassistenten nutzen diesen, um Suchanfragen oder Internetrecherchen durchzuführen.[9] Markprägend sind im Zusammenhang mit Smart-Speaker die amerikanischen Global Player Amazon und Google, die sind insgesamt 93 % des Marktes vereinnahmen.[10] Dabei fällt ein Marktanteil von 64 % auf Amazon und ein Anteil von 29 % auf Google.[11] Die stetig fortschreitende Digitalisierung hat auch in Deutschland zur Folge, dass ein Drittel aller Bundesbürger in ihrem Alltag bereits auf einen persönlichen Helfer zurückgreifen – die Tendenz ist steigend.[12] Digitale Sprachassistenten der Marktführer Amazon (Alexa)[13] und Google (Google Assistant)[14] sowie anderer Anbieter wie Apple (Siri)[15] oder asiatischer Hersteller, insbesondere Alibaba und Xiaomi, erobern die Lebensgestaltung der Menschen mehr und mehr.

Doch dem praktischen Nutzen steht entgegen, dass sämtliche elektronischen Geräte die Spuren ihrer Verwendung online oder auch offline vollkommen automatisch und vielmals vom Nutzer unbemerkt hinterlassen.[16] Neben den eigenen technischen Geräten, die entsprechende Daten an verwinkelten Orten des Betriebssystems abspeichern, sind es vor allen Dingen Suchmaschinen wie Google, die unaufhörlich sämtliche Suchanfragen, Themen und Schlagwörter der einzelnen Nutzer speichern.[17]

Über die Jahre dürften in großen Teilen der Bevölkerung die eigenen vier Wänden als Rückzugsort vor Außenstehenden, als Ort absoluter Privatheit, der eine höchstpersönliche Sphäre bereitstellt, angesehen worden sein. Doch der Einzug immer modernerer digitaler Technologien in den menschlichen Alltag droht diese Idylle einer geschützten Privatsphäre aufzuweichen. Auch wenn die Ermittlungsbehörden seit je her Möglichkeiten

---

8 Vgl. *Müller*, AG 2020, R270, R270.
9 Vgl. GfK-Studie Mastercard, vgl. https://www.presseportal.de/pm/113997/4417280 (zuletzt abgerufen am 31.10.2021); *Müller*, AG 2020, R270, R270.
10 *Miftari/Henrichs*, Zwischen innovativer Polizeiarbeit und neuem Managements, 297, 299.
11 https://www.golem.de/news/smarte-lautsprecher-apples-homepod-liegt-beim-marktanteil-hinter-alexa-und-co-1805-134455.html (zuletzt abgerufen am 31.10.2021).
12 Postbank Digitalstudie 2019, vgl. https://www.presseportal.de/pm/6586/4295010 (zuletzt abgerufen am 31.10.2021); GfK-Studie Mastercard, vgl. https://www.presseportal.de/pm/113997/4417280 (zuletzt abgerufen am 31.10.2021).
13 https://developer.amazon.com/de-DE/alexa (zuletzt abgerufen am 31.10.2021).
14 https://assistant.google.com/intl/de_de/ (zuletzt abgerufen am 31.10.2021).
15 https://www.apple.com/de/siri/ (zuletzt abgerufen am 31.10.2021).
16 *Michalke*, StraFo 2008, 267, 268.
17 *Michalke*, StraFo 2008, 267, 268.

zur Hand hatten, sich auch aus dem privaten Bereich Informationen zu beschaffen, so mag man sich doch fragen, ob es nun der Bürger selbst ist, der durch die Integration elektronischer Helfer in seinen Alltag die Möglichkeiten der Strafverfolgungsbehörden bedeutend vergrößert.[18]

Es lässt sich erahnen, dass mit dem Einzug smarter Assistenten in den Alltag der Bürger den Strafverfolgungsbehörden neue (heimliche und offene) Ermittlungsmöglichkeiten zur Verfügung stehen werden.[19] In dieser Arbeit soll untersucht werden, inwiefern diese Smart Speaker nach der aktuellen Gesetzeslage zu Zwecken der Strafverfolgung genutzt werden können. Dabei stellt sich die Frage, ob es hierfür neuer Ermächtigungsgrundlagen bedarf oder ein Zugriff auf diese Technologie de lege lata erfolgen könnte. Darüber hinaus gilt es zu untersuchen, welchen (praktischen) Problemen sich ein solcher Zugriff gegenübersehen kann und inwiefern sich ein solcher Zugriff auf Sprachassistenten mit der gängigen höchstrichterlichen Rechtsprechung zu ähnlich gelagerten Sachverhalten in Einklang bringen lässt. Im Anschluss an die Frage der Möglichkeiten eines strafprozessualen Zugriffs zur Beweismittelgewinnung soll in einem zweiten Schritt beleuchtet werden, welche verfassungsrechtlichen Bedenken oder strafprozessualen Besonderheiten hinsichtlich der Verwertbarkeit, der durch Smart Speaker erlangten Informationen auftreten können.

Schon seit mehreren Jahren nutzen die Strafverfolgungsbehörden die Möglichkeit auf informationstechnische Systeme zuzugreifen zur effizienteren Ausgestaltung ihrer Ermittlungstätigkeit. So konnte in der Vergangenheit bereits mehreren tausend Beschuldigten aufgrund der verwendeten IP-Adresse der Besuch von kinderpornografischen Websites nachgewiesen werden.[20] Bei den sich hieran anschließenden Hausdurchsuchungen stoßen die forensischen Experten bei der Auswertung der Festplatten zwar oftmals nicht mehr unmittelbar auf kinderpornografisches Bild- oder Videomaterial, stattdessen entdecken sie jedoch für den technischen Laien nicht mehr zugängliche Thumbnails, die auch dann zurückbleiben, wenn die einmal gespeicherten oder angesehenen Originalbilder gelöscht wurden.[21] Generell ist die Überwachung der Internetnutzung eine Ermittlungsmöglichkeit, der in den kommenden Jahren immer größere Bedeutung zu Teil werden wird. Das Aufrufen bestimmter Websites oder ent-

18 *Gless*, StV 2018, 671, 671.
19 *Miftari/Henrichs*, Zwischen innovativer Polizeiarbeit und neuem Managements, 297, 297.
20 *Michalke*, StraFo 2008, 287, 288.
21 *Michalke*, StraFo 2008, 287, 288.

sprechende Suchanfragen können als Indiz im Rahmen der Ermittlungen dienen und so Hinweise für die weitergehenden Ermittlungen liefern.[22] Die sog. Smart-Speaker können die Ermittlungsmöglichkeiten dabei auf verschiedene Arten erweitern. Beispielsweise könnte ein verzweifelter Nutzer den Sprachassistenten ansprechen und fragen, was er tun solle, wenn er eine bestimmte Straftat verübt habe. Auch wenn die technologischen Standards der sich heute auf dem Markt befindlichen Sprachassistenten ein Gespräch der Qualität von menschlicher Kommunikation noch nicht zulassen und der Sprachassistent auf entsprechend tiefergehende Anfragen noch antworten wird, dass er bei dieser Frage nicht helfen könne,[23] so dürfte es das Ziel der großen Anbieter sein, in den nächsten Jahren auch solch konstruktive Gespräche mit dem Sprachassistenten zu ermöglichen. Weiterhin ist denkbar, dass der Sprachassistent nach Informationen zu geplanten Straftaten (beispielsweise zum Bau einer Bombe) gefragt wird. Letztlich können sämtliche Informationsabfragen, denen ursprünglich am heimischen Computer via Google nachgegangen wurde, auch über einen Sprachassistenten ablaufen.

Realistischer und in der Praxis bereits vorgekommen ist jedoch, dass die Strafverfolgungsbehörden den Verdacht hegen, der Sprachassistent könnte Ausschnitte aus einem Gespräch aufgezeichnet haben, das in Verbindung zu einer Straftat stehen könnte.[24] Eine solche Situation trug sich im Jahr 2015 im amerikanischen Arkansas zu: Nach einem Leichenfund hatten die ermittelnden Beamten die Vermutung, dass ein im Wohnhaus vorhandener Sprachassistent Aufzeichnungen anfertigte, die nun Informationen zur Sachverhaltsaufklärung liefern könnten. Daher forderten die Ermittler Amazon zur Herausgabe, der auf deren Servern gespeichert Aufzeichnungen auf.[25] Da nicht auszuschließen ist, dass digitale Assistenten tatsächlich nur aufnehmen, was unmittelbar nach einem Code-Wort gesprochen wird und weil sie technisch vielfach noch nicht dazu in der Lage sind, Umgebungsgeräusche sauber herauszufiltern, sind sie mit Blick auf die Privatsphäre umstritten und für Strafverfolgungsbehörden bei Ermittlun-

22 Vgl. *Hiéramente*, StraFo 2013, 96, 97.
23 *Bager/Zota*, c´t 2016, Heft 26, 116, 117.
24 *Gless*, StV 2018, 671, 671.
25 *Kühl*, Bei Echo Mord?, https://www.zeit.de/digital/datenschutz/2016-12/amazon-echo-mord-aufnahmen-polizei/komplettansicht (zuletzt abgerufen am 31.10.2021); *Heller*, Alexa, war es Mord?, http://www.faz.net/aktuell/physik-mehr/internet-der-dinge-wenn-smarte-geraete-zu-zeugen-werden-15003037.html (zuletzt abgerufen am 31.10.2021).

gen interessant.[26] Auch in Deutschland wurden bereits Stimmen laut, die forderten im Rahmen eines Ermittlungsverfahrens auf sog. Smart Speaker zurückgreifen. So geht aus einer Beschlussvorlage des Landes Schleswig-Holsteins der Wunsch hervor, diese Daten und Informationen durch die Schaffung einer neuen Norm für die Aufklärung von Straftaten zukünftig zugänglich zu machen.[27] Im Rahmen der Innenministerkonferenz im Juni 2019 wurde dazu festgehalten, dass *„die Spurensicherung durch die Polizei in der digitalen Welt eine immer größere Bedeutung einnimmt. Im Rahmen der Strafverfolgung müssen die Behörden im Rahmen der geltenden Strafprozessordnung daher in der Lage sein, digitale Spuren zu erkennen, zu sichern und auszuwerten*"[28]. Gleichfalls wurde jedoch betont, dass die Strafverfolgung lediglich in der Lage sein müsse, solche digitale Spuren zu erkennen, zu sichern und auszuwerten, die *„aufgrund der heutigen rechtlichen Grundlagen bereits erhoben und gespeichert werden*"[29] dürfen. Hieraus lässt sich folgern, dass der gesetzgeberische Wille zum aktuellen Zeitpunkt nicht dahin gehen soll, neue strafprozessuale Befugnisnormen zu erlassen. Möglicherweise ist dies jedoch gar nicht erforderlich, da die Strafverfolgungsbehörden bereits nach der geltenden Rechtslage die von einem Sprachassistenten aufgezeichneten Audioaufzeichnungen nach § 100a StPO abfangen können. Zudem könnte in diesem Zusammenhang auch eine Online-Durchsuchung gem. § 100b StPO eine neuen Ermittlungsansatz darstellen. Darüber hinaus könnten die Mikrofone des Sprachassistenten als Wanze zur Ermöglichung einer Maßnahme nach § 100c StPO eingesetzt werden. Zuletzt könnte den Strafverfolgungsbehörden die Möglichkeit zu Teil werden, auf archivierte Audioaufzeichnungen im Rahmen einer Durchsuchung mitsamt anschließender Beschlagnahme gem. §§ 94 ff. StPO zuzugreifen.

Erstmals erlangten die Aufzeichnungen eines Smart Speakers in Deutschland in einem Strafprozess vor dem Landgericht Regensburg Ende des Jahres 2020 Bedeutung.[30] Im Prozess verwertete das Gericht unter anderem Aufzeichnungen des Smart Speakers Alexa. Unter anderem aus diesen Aufzeichnungen schloss das Gericht, dass sich der Angeklagte am

---

26 *Gless*, StV 2018, 671, 672.

27 *Krempl*, c´t 2019, Heft 14, 36.

28 Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 210. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 17.06.19, TOP 27 „Digitale Spuren", S. 18, https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/20190614_12/beschluesse.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 31.10.2021).

29 Ebd.

30 Vgl. LG Regensburg, Urteil vom 16. Dezember 2020 – Ks 103 Js 28875/19.

Tattag spätestens ab 23:54 Uhr in der Wohnung der Getöteten befand. Die Aufzeichnungen des Gerätes, welches als solches in der Wohnung der Getöteten sichergestellt worden war, wurden der Polizei von Amazon in Form einer per E-Mail übersandten Audio-Dateien übermittelt.[31] Mittels der kurzen, wenn auch nicht vollständig verständlich aufgezeichneten Sätze, stellte das Gericht fest, dass der Sprecher nicht lallte und seine Aussprache auch sonst nicht schwerfällig oder verwaschen war.[32] Ebenso schloss das Gericht aus dem Inhalt einer aufgezeichneten Äußerung des Angeklagten, dass das Tatopfer im Zeitpunkt der Aufzeichnungen am Tattag noch lebte. Aus der Tonsequenz ergab sich trotz des nicht vollständig verständlichen Inhalts, dass der Angeklagte mit dem späteren Tatopfer sprach.[33]

31 Vgl. LG Regensburg, Urteil vom 16. Dezember 2020 – Ks 103 Js 28875/19.
32 Vgl. LG Regensburg, Urteil vom 16. Dezember 2020 – Ks 103 Js 28875/19.
33 Vgl. LG Regensburg, Urteil vom 16. Dezember 2020 – Ks 103 Js 28875/19.

§ 2 Technischer Hintergrund

Unter einem Sprachassistenten (oder mobilen Assistenten) versteht man eine Software, die es dem Anwender ermöglicht mittels der eigenen menschlichen Sprache Informationen abzufragen oder Dialoge zu führen. Hierzu führt die Software eine Spracherkennung mitsamt Sprachanalyse durch, interpretiert und verarbeitet das Vernommene und formuliert als Ergebnis mittels Sprachsynthese eine Antwort.[34] Der Begriff des Sprachassistenten ist vom Begriff des Smart Speakers abzugrenzen. Während Sprachassistenten vielfach auch in anderen Technologien verbaut sind, wie beispielsweise der Sprachassistent Siri in Smartphones des Herstellers Apple[35], handelt es sich bei Smart Speakern um eigenständige physische Endgeräte deren Hauptfunktion die Beantwortung von Sprachbefehlen des Nutzers ist. Ein Smart Speaker stellt letztlich eine Untergruppe der Sprachassistenztechnologien dar. Der bekannteste sich heute auf dem Markt befindliche Smart Speaker ist Amazons „Alexa", der auch im Zentrum der hiesigen Arbeit steht. „Alexa" ist in diesem Zusammenhang jedoch lediglich der (Ruf)Name des „Kommunikationspartners" in Form künstlichen Intelligenz. Durch eben den Rufnamen „Alexa" wird der Smart Speaker aufgefordert, die Anfrage an den Sprachassistenten Alexa weiterzuleiten, damit dieser anschließend mittels seiner computergenerierten Stimme dem Nutzer die Antworten auf seine Anfragen übermitteln kann. Die einzelnen Smart Speaker des Herstellers Amazon tragen je nach Stil unterschiedlichste Namen (Amazon Echo, Amazon Echo Dot, Amazon Echo Studio) und sind in verschiedene Generationen je nach ihrem Herstellungsjahr und ihrer technischen Fortentwicklung unterteilt.[36]

34 Vgl. https://de.wikipedia.org/wiki/Intelligenter_pers%C3%B6nlicher_Assistent (zuletzt abgerufen am 31.10.2021).

35 https://www.apple.com/de/siri/ (zuletzt abgerufen am 31.10.2021).

36 Vgl. https://www.amazon.de/Echo-und-Alexa/b?ie=UTF8&node=10983902031 (zuletzt abgerufen am 31.10.2021).

A. Funktionsweise Smart Speaker

Zur Nutzung eines Smart Speakers muss der Kunde diesen zunächst einrichten, wozu es erforderlich ist, dass er beim jeweiligen Unternehmen, welches den Sprachassistenten bereitstellt, ein Kundenkonto anleget und den Sprachassistenten mit diesem Konto verknüpft.[37] Bei näherer Betrachtung eines Smart Speakers ist der Smart Speaker, der in der Wohnung des Betroffenen platziert ist, strikt vom übergeordneten Sprachassistenten zu trennen.[38] Bei einem Großteil der Smart Speaker beinhaltet dessen Gehäuse lediglich die Hardware, welche über eine Internetverbindung die Verknüpfung zum Sprachassistenten in den Rechenzentren der Anbieter herstellt.[39] Die Geräte in den Haushalten sind daher bloßer Zugang zum tatsächlichen Sprachassistenten. Der Smart Speaker ist lediglich für das Aufnahmen und Weiterleiten der gesprochenen Worte in die Cloud verantwortlich. In der Cloud übernimmt der Sprachassistent unter Zuhilfenahme der cloudbasierten künstlichen Intelligenz, die Verarbeitung der erhaltenen Informationen. Der Sprachassistent in Form der arbeitenden Cloud stellt daher das eigentliche Herzstück des technischen Systems dar. Damit der Zugang zur Cloud und damit die Weiterleitung „aktiviert" werden kann und die folgende Kommunikation zur Bearbeitung an die Server übertragen wird, ist es erforderlich, dass die in dem Smart Speaker verbaute Elektronik ununterbrochen mithört.[40] Nur so kann der Aktivierungscode erkannt werden und eine Verbindung zwischen dem Gerät und Rechenzentrum des Anbieters hergestellt werden. Das eine solche Verbindung zum Server besteht, erkennt der Nutzer meist an einem Signalton und einer leuchtenden LED.[41] Anschließend kommt der Spracherkennung mitsamt der notwendigen Verarbeitung der Aussagen des Nutzers eine entscheidende Bedeutung zu. Die der Spracherkennung zugrunde liegende Technologie basiert auf dem Zusammenspiel von vier Kerntechnologien.

---

37 *Winkemann*, CR 2020, 451, 451.

38 So ist hinsichtlich der Amazon Echo-Geräte, die häufig umfassend als „Alexa" bezeichnet werden, „Echo" die Bezeichnung für den Lautsprecher, mithin das Endgerät im Eigentum des Nutzers. Alexa hingegen bezeichnet die Software des Echo-Gerätes zur Spracherkennung und -analyse sowie zur Ausführung von Befehlen, vgl. *Miftari/Henrichs*, Zwischen innovativer Polizeiarbeit und neuem Managements, 297, 299.

39 *Hörner*, Marketing mit Sprachassistenten, S. 10 ff.

40 *Brockmeyer/Vogt*, Phänomenen des Big-Data Zeitalters, 187, 188; *Gless*, StV 2018, 671, 671.

41 *Mahn*, c´t 2019, Heft 11, 34, 34.

Die sog. Automated Speech Recognition (ASR) sorgt für die Umwandlung der Spracheingabe mittels verschiedener Algorithmen in eine computerlesbare Textform.[42] Dabei wird unter Heranziehung der Rechenleistung der Cloud mittels Natural Language Processing Techniken (NLP) den einzelnen Textfragmenten eine Bedeutung zugeordnet.[43] Hieran schließt sich der technische Prozess der Entscheidung und Durchführung zur Beantwortung der Anfrage an.[44] Nach der Verarbeitung der Befehle in der Cloud wird das Ergebnis mittels Text-to-Speech (TTS) wieder in eine Sprachausgabe umgewandelt und durch das Sprachrohr des Sprachassistenten in Form des Endgeräts akustisch wiedergegeben wird.[45] Text-to-Speech-Technologien arbeiten hauptsächlich mit konkatenierter (»verketteter«) Sprachsynthese, d. h. zur Versprachlichung eines Textes wird auf eine Datenbank mit kurzen Sprachaufnahmen (sog. Samples von maximal Silbenlänge) zurückgegriffen, die schließlich zu ganzen Worten verkettet werden.[46] Dieses baukastenartige Grundprinzip hat zur Folge, dass die so erzeugten Sprachausgaben hinsichtlich ihrer Natürlichkeit hinter menschlichen Sprachaufnahmen zurückbleiben.[47] Dank neuer, auf sogenannten Machine-Learning-Algorithmen beruhender Text-to-Speech-Technologien, hat die Sprachsynthese große Fortschritte gemacht. Künstliche Intelligenz

---

42 *Hörner*, Marketing mit Sprachassistenten, S. 11; *Warken*, NZWiSt 2017, 329; *Anke/Fischer/Lemke*, Digitalisierung von Staat und Verwaltung, 25, 27.

43 Unter NLP versteht man in der IT-Branche Techniken und Methoden zur maschinellen Verarbeitung natürlicher Sprache, mit dem Ziel eine direkte Kommunikation zwischen Mensch und Computer auf Basis der natürlichen Sprache zu ermöglichen, vgl. https://www.bigdata-insider.de/was-ist-natural-language-processing-a-590102/ (zuletzt abgerufen am 31.10.2021). Diese Techniken funktionieren auf Grundlage der Erkennung von ganzen Wörtern oder einzelnen Phonemen. Bei ersterer Methode werden auf dem Server ganze Wörter in vorgesprochener Form gespeichert und durchsucht den Speicher anschließend nach einem entsprechenden Wortmuster. Bei der genaueren phonemischen Spracherkennung wird hingegen jedes Wort in einzelne Phoneme unterteilt, vgl. https://www.itwissen.info/ASR-automatic-speech-recognition-Automatische-Spracherkennung.html (zuletzt abgerufen am 31.10.2021).

44 Deloitte, Studie Beyond Touch – Voice Commerce 2030, S. 16, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-business/CB_Studie_Beyond%20Touch.pdf (zuletzt abgerufen am 31.10.2021).

45 *Eberling*, Serverless mit Alexa, https://www.informatik-aktuell.de/betrieb/server/serverless-mit-alexa-skills-mit-aws-lambda-entwickeln.html#top (zuletzt abgerufen am 31.10.2021); *Anke/Fischer/Lemke*, Digitalisierung von Staat und Verwaltung, 25, 27; *Schult*, MMR 2020, 448, 450.

46 *Rammos/von Rosen*, ZUM 2020, 25, 25.

47 *Rammos/von Rosen*, ZUM 2020, 25, 25.

verleiht den Stimmen Rhythmus, sodass diese vielfach echt und menschlich klingen.[48] Insbesondere erfolgt die Versprachlichung der Texte dadurch eigenständig und ohne Rückgriff auf Samples.[49] Für die erfolgreiche Verarbeitung eines Sprachbefehls ist es grundsätzlich von entscheidender Bedeutung, dass der gesprochene Text akustisch bestmöglich wahrgenommen wird. Die ständige Weiterentwicklung des Systems ermöglicht es zudem immer mehr, dass die cloudbasierte künstliche Intelligenz eine kontextbezogene Interpretation der Anfrage gepaart mit dem Erkennen der Absicht des Kunden leisten kann.[50] Nach dem Abschluss eines solchen Vorgangs werden die aufgezeichneten Audioaufzeichnungen in der Cloud des Dienstleistungsanbieters gespeichert.[51] Sie können durch sämtliche Personen, die Zugang zur Cloud des Nutzers haben, abgehört und gelöscht werden.

Im Zuge der Verarbeitung eines Sprachbefehls kommt auch den sog. „Alexa-Skills"[52] eine besondere Bedeutung zu. Dabei handelt es sich um Möglichkeiten von Händlern und Herstellern, über den Sprachassistenten mit ihren Kunden in Kontakt zu treten. Die entsprechenden Unter-

---

48 *Wiegand*, c´t 2020, Heft 14, 118, 118.

49 *Rammos/von Rosen*, ZUM 2020, 25, 25.

50 Deloitte, Studie Beyond Touch – Voice Commerce 2030, S. 16, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-business/CB_Studie_Beyond%20Touch.pdf (zuletzt abgerufen am 31.10.2021).

51 Alexa Nutzungsbedingungen vom 17.12.2020 „*Alexa leitet Audiodaten in die Cloud, wenn Sie mit Alexa interagieren. Alexa lernt dabei und wird immer intelligenter […]. Um den Alexa Dienst zur Verfügung stellen zu können, zu personalisieren und um unsere Dienste zu verbessern, verarbeitet und speichert Ihre Alexa Interaktionen, wie Ihre Spracheingaben […]*", vgl. https://www.amazon.de/gp/help/customer/display.html?nodeId=201809740 (zuletzt abgerufen am 31.10.2021); vgl. ferner https://www.apple.com/de/legal/privacy/data/de/ask-siri-dictation/ (zuletzt abgerufen am 31.10.2021):
„Dein Anfrageverlauf wird über einen Zeitraum von bis zu sechs Monaten mit einer Zufalls-ID verknüpft. Dein Anfrageverlauf kann Transkriptionen, Stimmeingaben von Benutzer:innen, die sich zur Nutzung der Option „Siri & Diktierfunktion verbessern" bereit erklärt haben, Siri-Daten und zugehörige Anfragedaten wie Gerätespezifikationen, Gerätekonfiguration, Leistungsstatistiken und den ungefähren Standort deines Geräts zum Zeitpunkt der Anfrage enthalten. Nach sechs Monaten wird dein Anfrageverlauf von der zufälligen ID getrennt und kann für bis zu zwei Jahre gespeichert werden, um Apple dabei zu unterstützen, Siri, die Diktierfunktion und andere Funktionen zur Sprachverarbeitung, etwa die Sprachsteuerung, zu verbessern. Der kleine Teil der Anfragen, die geprüft wurden, kann über zwei Jahre hinaus ohne zufällige ID aufbewahrt werden, um Siri kontinuierlich zu verbessern."

52 Vgl. www.amazon.com/alexa-skills/b?ie=UTF8&node=13727921011 (zuletzt abgerufen am 31.10.2021).

nehmen schließen hierzu einen Vertrag mit den Anbietern von Smart Speakern und haben sodann die Möglichkeit, eigene Dienste für den Sprachassistenten zu entwickeln. Diese Anwendungen sind mit Apps auf Smartphones vergleichbar und werden im Kontext der Smart Speaker lediglich als Skills (Amazon) oder Action (Google) bezeichnet.[53] Sie erweitern den Smart Speaker somit um zusätzliche Funktionen. Die durch den Nutzer installierten Anwendungen werden sodann durch die Cloud zur gezielten Bearbeitung des Sprachbefehls herangezogen.[54] Hierzu muss der Entwickler (z.B. ein Essenslieferant, ein Wetterdienst, ein Radiosender) die App nach den Vorgaben der Plattform entsprechend programmieren (PaaS).[55] Je nach Anbieter des Smart Speakers muss der Nutzer den entsprechenden Skill installieren oder dieser ist losgelöst hiervon über die Cloud verfügbar. Aktiviert der Nutzer einen Skill sodann ebenfalls durch das entsprechende Aktivierungswort werden die dazugehörigen Informationen zwischen dem Dienstleistungsanbieter (beispielsweise Amazon) und dem Entwickler des Skills ausgetauscht. Wird eine Anfrage an den Sprachassistenten gerichtet, ohne dass der Nutzer den Namen eines bestimmten Skills nennt, versendet der Dienstleistungsanbieter den Inhalt der Anfrage an mehrere Skills. Aktiviert, ausgeführt und zur Beantwortung des Sprachbefehls herangezogen, wird letztlich der Skill, von welchem der Sprachassistent glaubt, dass er am besten geeignet ist.[56] Zukünftig soll versucht werden, das aktive Aktivieren eines bestimmten Skills gänzlich entbehrlich zu machen und die Anfragen der Nutzer alleine über den Konversationskontext einem bestimmten Skill zuzuweisen.[57]

Daneben kann nach ersten Entwicklungen auch auf Sprachassistenten zurückgegriffen werden, die ohne Übertragung, Verarbeitung und Speicherung der Daten in einer fremden Cloud auskommen. Dies hat den Vorteil, dass der Sprachassistent dann weder von einer funktionierenden Internetverbindung abhängig ist noch Audioaufzeichnungen das eigene

53 Deloitte, Studie Beyond Touch – Voice Commerce 2030, S. 18, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-business/CB_Studie_Beyond%20Touch.pdf (zuletzt abgerufen am 31.10.2021).

54 https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (zuletzt abgerufen am 31.10.2021).

55 *Schult*, MMR 2020, 448, 450.

56 *Schult*, MMR 2020, 448, 450.

57 Deloitte, Studie Beyond Touch – Voice Commerce 2030, S. 19; https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-business/CB_Studie_Beyond%20Touch.pdf (zuletzt abgerufen am 31.10.2021).

zu Hause verlassen würden.[58] Der Sprachassistent von des Unternehmen Snips[59] ermöglicht anstelle einer Speicherung und Verarbeitung über eine Cloud, eine Verarbeitung der Daten direkt über das jeweilige Gerät.[60] Mittels eines Raspberry Pi[61] erfolgt die Einrichtung des Offline-Sprachassistenten, der neben selbst programmierten Befehlen auch heruntergeladene Befehle umsetzen kann. Folglich kann im Vergleich zu einem Online-Sprachassistenten nicht derselbe Umfang an verarbeitbaren Sprachbefehle erwartet werden. Schwerpunktmäßig kommen solche Offline-Sprachassistenten daher vor allem in der Hausautomation zum Einsatz.[62] Dass die künstliche Intelligenz zudem direkt auf der Hardware des Endgerätes verortet ist, führt wiederum zu einer geringeren Leistungsfähigkeit des Sprachassistenten, der eben nicht auf die enormen Rechenleistungen eines Severs zurückgreifen kann. Die Antwortmöglichkeiten des Sprachassistenten sind dadurch begrenzt. Ebenso ist eine zügige Verarbeitung großer Datenmengen erschwert.[63]

B. Cloud Computing

Untrennbar, für den Nutzer jedoch unsichtbar, mit der Nutzung eines Smart Speakers verbunden ist dessen internetbasierte Verbindung an eine leistungsstarke Cloud, in der sämtliche Verarbeitungs-, Analyse- und Speichervorgänge ablaufen. Zum Verständnis der Funktionsweise eines Smart Speakers ist daher eine Auseinandersetzung mit dem der Technologie eines Sprachassistenten zugrunde liegenden Cloud-Computing notwendig.

Die mit der Globalisierung einhergehende immer weitläufigere Verbreitung von Sprachassistenten fordert auch die an diesem Prozess beteiligten Unternehmen immer stärker, die die bei der Nutzung der Technologien

58 *Jurran/Porteck*, c´t 2019, Heft 20, 72.

59 https://snips.ai/ (zuletzt abgerufen am 31.10.2021), aufgekauft durch „Sonos", vgl. https://investors.sonos.com/news-and-events/investor-news/latest-news/2019/Sonos-Announces-Acquisition-of-Snips/default.aspx (zuletzt abgerufen am 31.10.2021).

60 *Mahn*, c´t 2019, Heft 11, 34, 35.

61 Dabei handelt es sich um einen Mini-Computer, der vor allem auch Anfängern einen leichten Einstieg zum Programmieren ermöglicht, vgl. https://www.elektronik-kompendium.de/sites/com/1904221.htm (zuletzt abgerufen am 31.10.2021).

62 *Mahn*, c´t 2019, Heft 11, 34, 35.

63 Deloitte, Studie Beyond Touch – Voice Commerce 2030, S. 16 f., https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-business/CB_Studie_Beyond%20Touch.pdf (zuletzt abgerufen am 31.10.2021).

entstehenden Datenmengen effizient und gleichzeitig leistungsstark verarbeiten müssen. Da eine Datenverarbeitung lokal und direkt beim Dienstleistungsnutzer aus ökonomischen Gesichtspunkten nicht zielführend ist, hat sich die Auslagerung von Daten auf dezentrale Server durchgesetzt.[64] Insbesondere die Global Player der IT-Branche wie Amazon, Apple oder Google nutzen dies, um ihre informationstechnischen Dienstleistungen noch flexibler und mit größerer Skalierbarkeit auszugestalten.[65]

I) Definitionsansätze

Im Zuge dessen hat sich der Begriff des Cloud-Computing etabliert. Hierunter ist die Möglichkeit zu verstehen, Daten auf einem nicht lokal installierten Netzwerk zu speichern oder auf Anwendungen und Services zuzugreifen, die in der Cloud gespeichert sind.[66] Es handelt sich also um die Bereitstellung von IT-Infrastruktur und -Leistungen wie Speicherplatz, Rechenleistung oder Anwendungssoftware als Service über das Internet.[67] Die hierauf basierenden Anwendungen, Services oder abgelegten Daten können von überall aus aufgerufen und genutzt werden.[68] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert den Begriff des Cloud-Computing wie folgt:

> „*Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.*“[69]

64 *Niemann/Hennrich*, CR 2010, 686; *Giedke*, Cloud-Computing, S. 4 ff.
65 *Krischker*, Das Internetstrafrecht vor neuen Herausforderungen, S. 167 f.*;* *Weichert*, DuD 2010, 679, 679.
66 MüKoStGB/*Graf*, § 202a StGB, Rn. 96.
67 *Ogorek* in: BeckOK-GG, Art. 10 GG, Rn. 41.
68 Vgl. https://aixvox.com/cloud-computing-einfach-erklaert/?cn-reloaded=1 (zuletzt abgerufen am 31.10.2021).
69 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html (zuletzt abgerufen am 31.10.2021).

Zurückgehend auf die die Definition des NIST (National Institute of Standards and Technology) ist Cloud Computing ein Modell, das jederzeit und von überall über ein Netzwerk den Zugriff auf verschiedene Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) ermöglicht, die schnell und mit minimalem Aufwand zur Verfügung gestellt werden können.[70]

Im Detail lassen sich fünf wesentliche Eigenschaften des Cloud-Computing herausarbeiten. So läuft erstens die Bereitstellung der Ressourcen (z. B. Rechenleistung, Storage) automatisch und ohne Interaktion mit dem Service Provider ab (On-demand Self Service).[71] Zweitens sind sämtliche mit Standard-Mechanismen über das Netz abrufbar und nicht an einen bestimmten Client gebunden (Broad Network Access).[72] Drittens liegen die Ressourcen des Dienstleistungsanbieters in einem Pool gebündelt vor, aus dem sich die Nutzer bedienen können (Resource Pooling).[73] Viertens können die angebotenen Services sehr schnell und flexibel zur Verfügung gestellt werden, teilweise gar automatisch. Aus Anwendersicht scheinen die ihm zur Verfügung stehenden Ressourcen daher unendlich (Rapid Elasticity).[74] Zuletzt kann die Ressourcennutzung gemessen und überwacht werden und entsprechend in eingegrenzten Umfang den Cloud-Anwendern bereitgestellt werden (Measured Services).[75] Der Nutzer kann sich der Cloud-Dienstleistung jederzeit und ohne unmittelbare Kontaktaufnahme mit dem Diensteanbieter bedienen. Die Nutzung wird lediglich durch die eigene Interaktion initiiert, für die eine zweite Person nicht erforderlich ist. Wesentlich und unabdingbar für Cloud-Computing und dessen Nutzung ist dabei jedoch eine permanente Verknüpfung mit einem Netzwerk. Ohne Intra- oder Internetverbindung ist ein aktives Arbeiten mit der Cloud unmöglich. Ist diese Verbindung vorhanden, stehen dem Nutzer dagegen im Vergleich zur lokalen Datennutzung, bei welcher der Speicherplatz und die Rechnerkapazität begrenzt ist, theoretisch unbegrenzte Ressourcen zur Verfügung.[76]

---

70 *Mell/Grace*, The NIST Definition of Cloud-Computing, S. 2.
71 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html (zuletzt abgerufen am 31.10.2021).
72 Ebd.
73 Ebd.
74 Ebd.
75 Ebd.
76 *Kian*, Cloud Computing, S. 18.

Der entscheidende Unterschied um Cloud-Computing von herkömmlichen Technologien abzugrenzen, ist, dass die ganz überwiegenden Teile der Arbeits- und Speicherprozesse nicht mehr auf dem Endgerät des Benutzers, sondern auf den externen Cloud-Servern vorgenommen werden.[77] Im Unterschied zum herkömmlichen Outsourcing oder zum sog. Application Service Providing (ASP) unterscheidet sich Cloud Computing gleich mehrfach.[78] Am zugänglichsten ist dabei der Unterschied zum klassischen Outsourcing von IT-Dienstleistungen, bei welchem eine Verlagerung von IT-Infrastrukturen in ein bestimmtes Rechenzentrum stattfindet und dieses dort vom Dienstleister für den Auftraggeber betrieben wird. Der Kunde kann sodann durch einen remote access auf „seinen" Server im Rechenzentrum zugreifen.[79] Ähnlich ist die Situation auch beim *Application Service Providing*: Neben der zur Verfügung gestellten dedizierten Hardware in einem bestimmten Rechenzentrum wird dem Kunden zudem vom Application Service Provider eine auf seine individuellen Anforderungen zugeschnittene Anwendersoftware zur Nutzung überlassen.[80] Beim Cloud-Computing hingegen wird dem Kunden im Unterschied zu den gezeigten Möglichkeiten der Auslagerung bzw. Bereitstellung einer IT-Infrastruktur keine bestimmte Hardware mit einem bestimmten Speicherplatz zur Verfügung gestellt. Stattdessen nutzt der Kunde auf der vom Cloud Service Provider bereitgestellten Plattform einen virtueller Server. Diesen Server teilt sich der Kunde mit anderen Kunden, die die Dienste des Servers gleichwohl alle zur selben Zeit und ohne Überschneidungen nutzen können.[81] Die Vorteile dieser Arbeitsweisen liegen zum einen darin begründet, dass Softwareaktualisierungen vom Dienstleistungsanbieter zeitnah und zentral für alle Kunden durchgeführt werden können, ohne dass der Kunde gesondert Updates installiert muss. Zudem benötigt der Kunde weder eine besonders leistungsfähige Hardware noch eine besonders schnelle Internetverbindung, denn die konkrete Verarbeitung der Sprachbefehle

77 *Kian*, Cloud Computing, S. 19; *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.2, Rn. 1.
78 *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.2, Rn. 3.
79 *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.2, Rn. 3.
80 *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.2, Rn. 3.
81 *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.2, Rn. 3.

erfolgt auf leistungsfähigen Rechnern im Rechenzentrum.[82] Es ist lediglich eine Internetverbindung notwendig, über die die Audiodateien zur dezentralen Verarbeitung übertragen werden.

II) Ebenenstruktur

Obwohl nicht die „eine Art des Cloud-Computing" existiert[83], werden klassischerweise Speicherdienste wie Dropbox oder OneDrive als Synonym für die neuartigen Technologien des Cloud-Computing verstanden. Tatsächlich handelt es sich dabei jedoch lediglich um spezielle Ausprägungen des Cloud-Computing. In IT-Kreisen hat sich im Laufe der Zeit eine gängige Unterteilung des Cloud-Computing in aufeinander aufbauende Cloud-Ebenen etabliert.[84] Neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zieht auch das National Institute of Standards and Technology (NIST) die Unterteilung in Software as a Service (Saas), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) zur Verdeutlichung der einzelnen Teilaspekte des Cloud-Computing heran.[85]

1) IaaS Cloud-Computing

Die Basis der Cloud-Computing Modelle bildete die Infrastrukturebene. Durch sie werden diejenigen Dienste bereitgestellt, die auch ein lokaler Computer für einen ordnungsgemäßen Betrieb bereitstellen müsste.[86] Bei den sog. IaaS-Angeboten (Infrastructure as a Service) greift der Kunde auf IT-Infrastrukturen des Anbieters, wie Rechenleistung oder Speicherplatz zurück.[87] Während der Dienstleistungsanbieter für den Betrieb und die

82 *Heydn*, MMR 2020, 435, 435.
83 *Hennrich*, CR 2011, 546, 546; *Hornung/Sädtler*, CR 2012, 638, 638.
84 *Kian*, Cloud-Computing, S. 20; *Lehmann/Giedke*, CR 2013, 608, 609; *Nägele/Jacobs*, ZUM 2010, 281, 282; *Federrath*, ZUM 2014, 1, 2; *Böse/Rockenbach*, MDR 2018, 70.
85 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html (zuletzt abgerufen am 31.10.2021); *Mell/Grace*, The NIST Definition of Cloud-Computing, S. 2 f.
86 *Barnitzke*, Rahmenbedingungen des Cloud-Computing, S. 48.
87 *Niemann/Paul*, K&R 2009, 444, 445; *Hennrich*, CR 2011, 546 f.; *ders*., Cloud Computing, S. 63; *Westerfeld* in: Niemann/Paul, Praxishandbuch Rechtsfragen des Cloud Computing, S. 9 Rn. 7.

Konfiguration der Infrastruktur verantwortlich ist, verwendet der Nutzer das ihm vom Anbieter zur Verfügung gestellte Betriebssystem, worauf er individuell seine benötigte Software installiert.[88] Der Cloud-Nutzer ist daher selbst für das Konfigurieren des Betriebssystems und das Installieren von Anwendungen verantwortlich.[89] Er wird auf der ihm zur Verfügung gestellten Datenspeicher als virtualisierten und in hohem Maß standardisierten Dienst seine eigene Services zum internen oder externen Gebrauch aufbauen. So kann der Cloud-Kunde unter Zuhilfenahme der angemieteten Rechenleistung, Arbeitsspeicher oder Datenspeicher ein Betriebssystem mit Anwendungen seiner Wahl anwenden.[90] In diesem Zusammenhang sind beispielsweise die Bereitstellung von Rechenplatz und Onlinespeicher über die Amazon Web Services oder die bekannten Speicherdienste wie Google Drive oder Dropbox zu nennen.[91] Auch Anbieter von Music-Clouds, die einen Speicherort für Musik zur anschließenden Widergabe oder Weitergabe durch Links zur Verfügung stellen, zählen zu den IaaS-Angeboten. Anstelle einer lokalen Speicherung der Audiodateien auf dem lokalen Endgerät, können zuvor hochgeladene und sodann extern gespeicherte Audiodateien zu einem späteren Zeitpunkt gestreamt werden.[92]

2) PaaS Cloud-Computing

Auf der PaaS (Platform as a Service) Ebene wird dem Kunden eine Softwareumgebung zur Verfügung gestellt, mittels derer er selbst eigene Anwendungen entwickeln oder bestehende Anwendungen erweitern kann. Hierbei muss es sich nicht zwangsläufig um Anwendungen zur eigenen Benutzung handeln. Ebenso sind auch Applikationen, die anderen Cloud-Nutzern mit Hilfe der Cloud-Infrastruktur des PaaS-Anbieters zur Verfü-

88 *Brennscheidt*, Cloud Computing und Datenschutz, S. 32; *Birk/Wegener*, DuD 2010, 641, 642; *Kroschwald*, Informationelle Selbstbestimmung in der Cloud, S. 12.

89 *Schmid*, Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen, S. 49.

90 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html (zuletzt abgerufen am 31.10.2021); *Rafsendjani* in: Bräutigam, IT-Outsourcing und Cloud-Computing, Teil 3, A., Rn. 7; *Bierekoven*, ITRB 2010, 42, 43.

91 *Kian*, Cloud-Computing, S. 21; *Schmid*, Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen, S. 49; *Müller*, Cloud-Computing, S. 53.

92 *Hansen*, c/t 2011, Heft 23, S. 98 f.

gung gestellt werden denkbar.[93] Im Zuge der Möglichkeit, selbst neue Applikationen in der Cloud zu entwickeln, liegt für den Kunden der entscheidende Vorteil darin, dass er hierfür nicht auf eigene Rechenleistung angewiesen ist, sondern seine entwickelte Software über die Cloud des Anbieters testen und optimieren kann.[94] Ein solches Angebot richtet sich folglich primär an Entwickler und nicht den normalen Endkunden.[95] Das Entwickeln solcher Anwendungskomponenten ermöglicht es Unternehmen diese an seine Geschäftsabläufe anzupassen und so seinem Kunden auch die Kontaktaufnahme via Cloud-Services anbieten zu können.[96] Auch bei den von Amazon verkauften Smart Speaker ist es möglich, mittels Amazon Voice Services dem eigenen Gerät eine Schnittstelle hinzuzufügen und so eine Sprachsteuerung, Alexa-Skills und die Integration von Smart-Home-Features selbst zu programmieren.[97]

3) SaaS Cloud-Computing

SaaS-Angebote (Software as a Service) ermöglichen dem Nutzer die Verarbeitung von Daten über die bereitgestellte Software ausschließlich über den Internetbrowser oder einen anderen Client.[98] Bei dieser Anwendungsart handelt es sich für die breite Masse an Nutzern als Endnutzer um die interessanteste Anwendung.[99] Dabei sind die Softwareanwendungen lediglich auf der Infrastruktur des Anbieters installiert[100] Der Kunde erhält die komplette Anwendung als Dienst zur Verfügung gestellt, wobei der Anbieter sowohl die Infrastruktur als auch die jeweiligen Softwareangebo-

93 *Müller*, Cloud Computing, S. 55.
94 *Birk/Wegener*, DuD 2010, 641, 643; *Süptitz/Utz/Eymann*, DuD 2013, 307, 308; *Schmidl*, IT-Recht, S. 54 f.
95 *Bell*, Strafverfolgung in der Cloud, S. 29; *BITKOM*, Evolution in der Technik, S. 26.
96 *Giedke*, Cloud Computing, S. 30.
97 *Schult*, MMR 2020, 448, 450.
98 *Schmidt-Bens*, Cloud Computing Technologien und Datenschutz, S. 16.
99 *Schorer* in: Hilber, Handbuch Cloud Computing, Teil 1C, Rn. 25; *Federrath*, ZUM 2014, 1, 2.
100 *Bell*, Strafverfolgung in der Cloud, S. 29; *Nägele/Jacobs*, ZUM 2010, 281, 282; *Heydn*, MMR 2020, 435; *Hentschel/Leyh* in: Reinheimer Cloud-Computing, 3, 11; *Sujecki*, K&R 2012, 312, 313; *Westerfeld* in: Niemann/Paul, Praxishandbuch Rechtsfragen des Cloud Computing, S. 9, Rn. 9; *Grenzer/Heitmüller*, PinG 2014, 221, 222.

te und Anwendungen verwaltet.[101] Ohne weiteres eigenes Zutun kann der Kunde die ihm zur Verfügung gestellte Software in der Cloud ausführen und nutzen.[102] Bei der Nutzung der bereitgestellten Software über seinen Internetbrowser ist sodann keine dauerhafte oder vorübergehende Speicherung oder Installation auf seinem Rechner erforderlich.[103] Klassische Beispiele hierfür sind die Nutzung eines E-Mail Kontos bei den gebräuchlichen Anbietern web.de, Google oder gmx.de[104], die Nutzung von „Google Maps"[105] oder der sozialen Netzwerke wie Facebook, Twitter, LinkedIn und Xing.[106]

4) FaaS-Cloud Computing

Neben den drei gängigen Ebenen handelt es sich bei Function as a Service (FaaS) um eine weitere Kategorie des Cloud Computing. Dabei stellt der Anbieter einzelne Funktionen bereit, die bei Nutzung durch der den Kunden innerhalb kurzer Zeit ein Ergebnis präsentieren. Hierbei werden Komponenten wie Server, Netzwerk, Speicher, Betriebssystem, Daten und die Anwendung selbst durch den Cloud-Betreiber bereitgestellt. Dennoch bleibt die Infrastruktur des Services und die Server dem Nutzer unbekannt.[107] Bei FaaS handelt es sich um reaktive Prozesse, die von entsprechenden „Triggerevents" ausgelöst und gesteuert werden.[108] Laufende Prozesse existieren hingegen nicht. Erst durch einen bestimmten Trigger wird eine spezifische Funktion in Gang gesetzt. Function as a Service ermittelt sodann das Ergebnis und wartet anschließend auf den nächsten Aufruf.[109]

Im Unterschied zu PaaS, das mehrere Requests gleichzeitig bedient, wird bei FaaS eine einzelne Funktion aufgerufen und binnen Millisekun-

101 *Grünwald/Döpkens*, MMR 2011, 287; *Niemann/Paul*, K&R 2009, 444, 445.
102 *Busching*, Der Schutz privater Informationen bei Cloud Computing, S. 29.
103 *Brennscheidt*, Cloud Computing und Datenschutz, S. 35; *Rafsendjani* in: Bräutigam, IT-Outsourcing und Cloud-Computing, Teil 3, A., Rn. 9; *Hennrich*, CR 2011, 546, 547.
104 *Schorer* in: Hilber, Handbuch Cloud Computing, Teil 1C, Rn. 25.
105 *Hennrich*, Cloud Computing, S. 70.
106 *Müller*, Cloud Computing, S. 58.
107 Vgl. *Luber/Karlstetter*, Was ist Function as a Service (FaaS)?, https://www.cloudcomputing-insider.de/was-ist-function-as-a-service-faas-a-758571/ (zuletzt abgerufen am 31.10.2021).
108 Ebd.
109 Ebd.

den beantwortet. Dagegen stehen bei PaaS-Anwendungen mehrere Anfragen innerhalb eines Prozesses im Vordergrund, die wesentlich mehr Zeit in Anspruch nehmen.[110]

III) Einordnung eines Sprachassistenten in Form eines Smart Speakers

Die verschiedenen Servicemodelle unterscheiden sich primär im Einfluss des Kunden auf die Sicherheit der angebotenen Dienste. Während bei IaaS-Modellen der gesamte Bearbeitungsvorgang innerhalb des Verantwortungsbereichs des Kunden abläuft und dieser so die Kontrolle über das IT-System mitsamt des Betriebssystems behält, besitzt er bei PaaS-Anwendungen nur eine eingeschränkte Kontrollmöglichkeit der Anwendungen. Bei SaaS-Modellen liegt schließlich die komplette Kontrolle in den Händen des Dienstleistungsanbieters.[111] Bei der Nutzung eines Smart Speakers handelt es sich danach nicht um das klassischste Feld des Cloud-Computing in Form der gewollten Datenspeicherung mittels Anwendungen wie Dropbox, iCloud oder Google Drive,[112] sondern um die Inanspruchnahme von Rechenleistung des Servers zur Ausführung der Sprachbefehle. Dabei handelt es sich um ein klassisches Beispiel für die Anwendung von Function as a Service. Bei einer Anfrage an einen Sprachassistenten liefert diese ein in sich abgeschlossenes Ergebnis. Nach der Bereitstellung des Ergebnisses ist die Funktion direkt wieder ansprechbar und befindet sich im gleichen Ausgangszustand.[113] Obwohl FaaS zustandslos ist, ist eine Speicherung der Daten durch eine mit FaaS verbundene (Cloud-)Datenbank möglich und üblich.[114] Die Speicherung erfolgt im Unterschied zu den genannten Fällen des Cloud-Storage, einer Unterkategorie des Cloud-Computing, nicht zur Aufbewahrung für den Nutzer, sondern zur Verbesserung der eigenen Dienstleistungen des Dienstleistungsanbieters. Im Unterschied zum Cloud-Storage ist es daher auch nicht der Nutzer, der aktiv bestimmt, dass seine Daten in einer solchen Cloud gespeichert

110 Ebd.
111 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html (zuletzt abgerufen am 31.10.2021).
112 Vgl. nur *Pötters/Werkmeister*, JURA 2013, 5, 8.
113 Vgl. *Luber/Karlstetter*, Was ist Function as a Service (FaaS)?, https://www.cloudcomputing-insider.de/was-ist-function-as-a-service-faas-a-758571/ (zuletzt abgerufen am 31.10.2021).
114 Ebd.

werden. Bei der Nutzung eines Sprachassistenten ist diese Speicherung vielmehr ein Nebeneffekt, der mit der Nutzung der Dienstleistung einhergeht.

IV) Erscheinungsformen Cloud-Computing

Üblicherweise wird das Cloud-Computing in vier Bereitstellungsmodelle (namentlich Public Cloud, Private Cloud, Community Cloud und Hybrid Cloud) unterteilt.[115] Für eine Private Cloud ist kennzeichnend, dass diese nur für eine Institution betrieben wird.[116] Ob die Privat Cloud von der Institution selbst (On-promise-Private Cloud) oder einem Dritten (Managed Private Cloud) organisiert und geführt wird ist unerheblich.[117] Dabei bedeutet privat jedoch nicht, dass die Server im Eigentum der Institution stehen oder die Institution Betreiber der Server ist. Privat verdeutlicht in diesem Zusammenhang lediglich, dass die Institution die konkrete Cloud allein nutzt und kontrolliert.[118] Für eine erhöhte Sicherheit sorgt dabei nicht zuletzt, dass sämtliche Nutzerdaten im eigenen (Unternehmens-) Netzwerk verbleiben und sämtliche Datensicherungsmaßnahmen eigenverantwortlich umgesetzt werden können.[119] Die Schattenseite hiervon sind kostenintensive Anschaffungen, die im Bau eines eigenen Rechenzentrums, entsprechenden Investitionen in Hardware und sonstige Infrastruktur oder in den durchlaufenden Verwaltungskosten liegen können.[120]

Im Gegenteil dazu bezeichnet man als Public Cloud, Cloud-Angebote, bei denen die Anbieter (z.B. Amazon, Apple, Google, Microsoft) und die potenziellen Benutzer nicht derselben organisatorischen Einheit an-

---

115 *Schuster/Reichl*, CR 2010, 38, 38; *BITKOM*, Evolution in der Technik, S. 31; *Heidrich/Wegener*, MMR 2010, 803, 803.

116 *Müller*, Cloud Computing, S. 41; *Schuster/Reichl*, CR 2010, 38, 38; *Giebichenstein*, BB 2011, 2218, 2218.

117 *Bedner*, Cloud Computing, S. 33.

118 *Pohle/Ammann*, CR 2009, 273, 274; anders ist dies bei der sog. Internal Cloud, bei der die gesamte Cloud-Infrastruktur im Eigentum der Institution steht und von dieser auch selbst betrieben wird, wie dies beispielsweise bei einem Unternehmensintranet in Cloud-Form der Fall ist. Daraus folgt, dass eine Internal Cloud stets eine Private Cloud ist, eine Privat Cloud jedoch nicht automatisch eine Internal Cloud ist, *Giebichenstein*, BB 2011, 2218; vgl. zum Gesamten *Bedner*, Cloud Computing, S. 33.

119 *Müller*, Cloud Computing, S. 42 f.

120 *Barnitzke*, Rahmenbedingungen des Cloud-Computing, S. 54; *Niemann/Paul*, K&R 2009. 444, 445.

gehören. In einer solchen Cloud können die von einem Anbieter zur Verfügung gestellten Dienste von der Allgemeinheit oder einer großen Gruppe genutzt werden.[121] Es kann durch den Anwender daher auch nicht mitbestimmt werden, mit welchen weiteren Nutzern er sich die Hardware teilt.[122] Ebenso wenig kommt dem Nutzer ein gewisser Gestaltungsspielraum für Kontrolle, Weisungen und individuelle Serviceleistungen zu.[123] Zudem fehlt es dem Kunden oftmals an datenschutzrechtlichen- oder IT-sicherheitsrelevanten Informationen wie beispielsweise einer Übersicht über sämtliche Orte der Datenverarbeitung oder einer Bescheinigung über die Einhaltung von IT-Sicherheitsvorgaben.[124] Über eine Hybrid Cloud können schließlich mehrere Cloud-Infrastrukturen gemeinsam genutzt werden. Insoweit handelt es sich dabei um eine Mischform zwischen einer Private Cloud und der Public Cloud. Während ein Teil der Daten und Dienste in öffentliche Clouds ausgelagert werden, bliebt der übrige Teil unternehmensinternen Private Clouds vorbehalten. Unter sicherheitstechnischen Gesichtspunkten hat dies den Vorteil, dass das Unternehmen entscheiden kann, ob es sensible Daten in der Private Cloud speichert und im eigenen Kontrollbereich belässt und weniger schützenswerte Daten in die Public Cloud auslagert, umso auch besser mit eventuell auftretende Lastspitzen umgehen zu können.[125]

C. Nutzen und Risiken

Der größte Vorteil vieler Cloud-Lösungen liegt darin, dass die Beschaffung eigener Hard- und Software für die Kunden obsolet wird und ihnen dadurch ein enormes wirtschaftliches Einsparpotential zukommt. Primär kommt dieses Phänomen im Zusammenhang mit der Business Cloud zum Tragen, bei der Unternehmen eine Vielzahl an Computer Ressourcen zügig und mit minimalem Verwaltungsaufwand bereitgestellt werden können. Diese Unternehmen müssen nicht mehr in eigene IT-Infrastruk-

121 *Braun/Kunze/Nimis/ Tai*, Cloud Computing, S. 27 f.; *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 3, Rn. 323; *Schröder/Haag*, ZD 2011, 147, 148.

122 *Cornelius*, StV 2016, 380.

123 *Maisch/Seidel*, VBlBW 2012, 7, 8; *Hennrich*, CR 2011, 546, 547; *Haas/Hofmann*, Risiken aus der Cloud, S. 6; *Lindner/Niebler/Wenzel*, Der Weg in die Cloud, S. 17.

124 *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, S. 23.

125 *Bedner*, Cloud Computing, S. 34 f.; *Braun/Kunze/Nimis/ Tai*, Cloud Computing, S. 29.

turen investieren, sondern lediglich für die Menge an Speicherplatz oder Rechnerkapazitäten bezahlen, die tatsächlich benötigt wird und können alle Daten für sämtliche Berechtigte jederzeit und von überall verfügbar machen.[126] Daneben hält das Cloud-Computing auch für private Nutzer diverse Vorzüge bereit, die in verschiedensten täglichen Aktivitäten zum Vorschein kommen. Zu den ersten Anwendungen, die in der Cloud zur Verfügung gestellt wurden, zählten neben sog. Webmail Dienste wie gmail oder webmail auch Dienste zur generellen Speicherung von Musik, Fotos und anderen Dateien (Dropbox, Google Drive oder Microsoft Sky Drive).[127] Ebenfalls auf Grundlage der Cloud-Technologien arbeiten Musik- und Filmstreamingdienste wie Spotify oder Netflix.[128] Dabei profitieren auch private Nutzer von der Möglichkeit, unabhängig von Ort und Zeit auf ihre Inhalte zugreifen zu können, ohne hierfür einen lokalen physischen Speicher zu benötigen. Systemabstürze auf Seiten des Verbrauchers lassen die Daten in der Cloud unberührt und trotz eines wenig leistungsfähigen Rechners können komplexe Softwareanwendungen aufgrund der Cloudunterstützung genutzt werden.[129]

Nun handelt es sich bei Sprachassistenten weder um cloudbasierte Technologien, die primär der Speicherung diverser Dateien dienen noch um Streamingdienste, sondern persönliche Assistenten, die bei Fragen aller Art als Ansprechpartner fungieren und unter Verwendung der Cloudkapazitäten Antworten auf diese Fragen bereithalten. Als ständiger Begleiter stehen die Sprachassistenten ihren Nutzern rund um die Uhr zur Verfügung. Diese permanente Verfügbarkeit hat jedoch auch zur Folge, dass die Ohren des Sprachassistenten in Form des Smart Speakers ununterbrochen ihre Umgebung nach dem Aktivierungswort (oder ähnlich klingenden Lauten) „belauschen". Gleich ob der Sprachassistent bewusst oder unbewusst aktiviert wurde, speichert dieser die vernommenen Informationen rund um die Uhr in der Cloud des Dienstleistungsanbieters.[130] In

126 *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.2, Rn. 2; *Bieber/Schröder* in: Niemann/Paul, Praxishandbuch Rechtsfragen des Cloud Computing, S. 43, Rn. 19 f.

127 *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.1, Rn. 9.

128 *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.1, Rn. 9.

129 *James* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 11.1, Rn. 9.

130 *Blechschmitt*, MMR 2018, 361, 362; vgl. auch *Heidrich/Maekeler*, c´t 2017, Heft 22, 86, 86; *Bleich*, c´t 2019, Heft 1, 16, 18.

diesem Zusammenhang gaben auch Amazon und Apple zu, dass ihre Mitarbeiter die aufgezeichneten Audiodateien nachträglich abhören, um die Arbeitsweise und Spracherkennung der Programme zu optimieren.[131] Laut Google handle es sich dabei jedoch lediglich um rund 0,2 Prozent der Aufzeichnungen. Apple und Amazon zufolge sind es jedenfalls weniger als ein Prozent.[132] Ferner birgt das Erfordernis eines permanenten Zuhörens denklogisch Risiken für den Nutzer. Beispielsweise dann, wenn Amazons Sprachassistent Alexa mithört, obwohl er dies gar nicht sollte und der Benutzer hiervon auch keine Kenntnis hatte. Die Ursachen hierfür können unterschiedlicher Art sein. Insbesondere ist daran zu denken, dass das System fehlerhaft davon ausgeht, aktiviert worden zu sein, da es einen ähnlich klingenden Begriff (beispielsweise die Rufnahmen Alexander oder Alexandra) mit dem eigentlichen Aktivierungswort verwechselte.[133]

Darüber hinaus sind Fälle bekannt, in welchen Nutzern auf Grundlage ihres datenschutzrechtlichen Auskunftsanspruchs gem. Art 15 DSGVO Auskunft über die von ihnen gespeicherten Daten verlangten. Bei einer solchen Anfrage an Amazon erhielt der Anfragende neben ca. 50 Dateien, die auf seine Person bezogene Daten enthielten (bspw. Suchverläufe) auch ca. 1700 WAV-Dateien sowie eine PDF-Datei, die Transskripte über die Aufzeichnungen des Sprachassistenten enthielten. Bei diesen Audioaufzeichnungen handelte es sich jedoch um Alexa-Sprachaufzeichnungen eines fremden Amazon-Kontos, die fälschlicherweise falsch zugeordnet wurden.[134] Zu den cloudspezifischen Risiken zu zählen ist auch, dass aufgrund der räumliche Trennung zwischen Anwender und Server-Standorten dieser regelmäßig keine Kenntnis darüber besitzt, auf welchen Systemen sich die Daten in einem bestimmten Zeitpunkt befinden. Weitergedacht erschwert dies eine überprüfbare Löschung der Daten.[135] Dies gilt nicht nur während der laufenden Nutzung der Cloud, sondern auch nach Beendigung des entsprechenden Nutzungsvertrages, worauf der Cloud-Anbieter die Daten des Cloud-Nutzers aufgrund des Zweckbindungsgrundsatzes nach § 20 Abs. 2 Nr. 2 BDSG löschen müsste, da eine fortlaufenden Speicherung der Daten (auch zum Zwecke der Systemverbesserung hin-

131 Vgl. *Barczok*, c´t 2019, Heft 10, 35, 35.
132 *Jurran*, c´t 2019, Heft 18, 36, 36.
133 *Blechschmitt*, MMR 2018, 361, 362; *Jurran*, c´t 2018, Heft 23, 68; *Moll/Rusch-Rodosthenous*, Amazon Alexa – ein Reaktionscheck, S. 16.
134 *Bleich*, c´t 2019, Heft 1, 16, 16.
135 *Schröder/Haag*, ZD 2011, 147, 150.

sichtlich des konkreten Nutzers) sodann nicht mehr erforderlich ist.[136] Der ehemalige Cloud-Nutzer kann jedoch nicht nachvollziehen, ob der Cloud-Anbieter die Daten und sämtliche Backups tatsächlich vollständig gelöscht hat.[137] Mit der Nutzung eines Cloud-Dienstes geht schließlich einher, dass der Nutzer das Vertrauen hinsichtlich der Aufbewahrung und des Schutzes der Daten gewissermaßen in die Hände Dritter gibt.[138] Dadurch bleiben Bedenken hinsichtlich der Einhaltung des Datenschutzes sowie die Angst des Verwenders, ob Dritte in den Besitz der Daten gelangen könnten.[139]

136 *Schmid*, Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen, S. 64.
137 *Schmid*, Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen, S. 64.
138 *Brookmann*, ZD 2012, 401.
139 *Lindner/Niebler/Wenzel*, Der Weg in die Cloud, S. 17.

§ 3 Elektronische Daten im Strafverfahren

Einhergehend mit der stetig wachsenden Bedeutung digitaler Medien, seien es Foto-, Video- oder Audioaufnahmen, die auf Speichermedien wie Computern, Handys, Servern und in der Cloud gespeichert werden,[140] steigt auch deren Bedeutung für den Strafprozess.[141]

A. Ziel des Strafverfahrens

I) Allgemeines

Die Wahrheit über eine behauptete oder für möglich gehaltenen Straftat zu ermitteln und den Täter der gesetzlichen Rechtsfolge zuzuführen, ist das primäre Ziel des Strafverfahrens.[142] Der in § 244 Abs. 2 StPO normierte Begriff der Wahrheit wird dabei gemeinhin als Übereinstimmung von Vorstellung und Wirklichkeit verstanden.[143] Erkenntnistheoretisch gründet dies auf einem korrespondenztheoretischen Wahrheitsverständnis, nach der Wahrheit die Übereinstimmung der Erkenntnis mit einem außerhalb ihrer selbst liegenden Gegenstand bedeutet.[144] Die Suche nach der Wahrheit prägt das gesamte Ermittlungsverfahren, das darauf ausgelegt ist, durch das Erforschen der materiellen Wahrheit schließlich auch Gerechtigkeit zu entfalten.[145] Durch die im deutschen Strafprozess geltende Amtsermittlungspflicht aus § 244 Abs. 2 StPO ist das Gericht verpflichtet den Sachverhalt unabhängig vom Prozessverhalten der Verfahrensbeteiligten von Amts wegen aufzuklären. Dadurch soll der durch die Zuwiderhandlung gegen ein durch das materielle Recht geschütztes Rechtsgut entstandene Konflikt aufgelöst und so die Erhaltung des Geltungsanspruchs

140 *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, 173, 175.
141 Vgl. *Singelnstein* in: Big Data – Regulative Herausforderungen, 179, 179.
142 BGHSt 1, 94, 96; *Fischer* in: KK-StPO, vor § 1 StPO, Rn. 3; *Kudlich* in: MüKo-StPO, Einl., Rn. 7.
143 *Trüg/Habetha* in: MüKo-StPO, § 244 StPO, Rn. 47; FS-Böttcher/*Trüg/Kerner*, 191, 192 ff.
144 *Theile*, NStZ 2012, 666,666.
145 *Trüg*, ZStW 2008, 331, 335; FS-Böttcher/*Trüg/Kerner*, 191, 192 ff.; *Malek*, StV 2011, 559, 560.

des materiellen Strafrechts gesichert werden.[146] Mithin wird der im Einzelfall entstandene Strafanspruch gegenüber dem Einzelnen auf diese Weise durch das Strafverfahren durchgesetzt.[147] Das Streben nach einer gerechten Entscheidung bedeutet jedoch nicht, einseitig die Durchsetzung des Strafanspruchs zu priorisieren, sondern ebenso die Rechtmäßigkeit der Entscheidung, unter Beachtung der Rechte des Betroffenen, zu garantieren.[148] Die Wahrung dieser Rechte, die verfassungsrechtlich in Art. 20 Abs. 3 GG sowie unionsrechtlich in Art. 6 EMRK und dem hieraus abgeleiteten „Fair-Trial" Grundsatz verankert sind, sollen eine womöglich „richtige", aber nicht rechtmäßig entstandene Entscheidung zum Schutz des Rechtsstaates verhindern. Der rechtsstaatliche Anspruch an eine rechtmäßig zustande gekommene Entscheidung schränkt folglich das vorab benannte Primärziel des Strafverfahrens wieder ein. Dennoch zieht ein nicht rechtmäßig erlangtes Beweismittel nicht zwangsläufig ein Beweisverbot nach sich. Dies belegt nicht zuletzt die Theorienvielfalt, die zur Entstehung eines unselbstständigen Beweisverwertungsverbots herangezogen wird.[149] Die Frage nach dem Verhältnis zwischen der Wahrheitsfindung auf der einen und der Rechtsstaatlichkeit auf der anderen Seite mündet also stets in einem Spagat, der auch im Laufe dieser Arbeit noch seinen Platz einnehmen wird. Jedenfalls eine Wahrheitserforschung um jeden Preis ist dem deutschen Strafprozess fremd.[150] Im Gesamten zielt das Strafverfahren dabei keinesfalls lediglich auf die Bestrafung des Täters ab, sondern richtet den Blick auch auf den Menschen, der durch die Straftat zum Opfer wurde. Dem Opfer selbst wird durch das Strafverfahren ein Justizgewährleistungsanspruch, als Ausfluss des Rechtsstaatsprinzips zu Teil,[151] der den mit der Entscheidung einherkommenden Rechtsfrieden in seiner Wertigkeit fördern soll.[152]. Nicht zuletzt um Privatrachen und Selbstjustiz zu verhindern, hat der Gesetzgeber die Strafverfolgung in die

146 *Kühne*, Strafprozessrecht, Rn. 1; *Ostendorf*, Strafprozessrecht, Rn. 7; *Rieß*, JR 2006, 269, 272.

147 BVerfGE 20, 45, 49; *Kindhäuser/Schumann*, StPO, § 1, Rn. 1; *Heger/Pohlreich*, Strafprozessrecht, Rn. 14.

148 *Beulke/Swoboda*, Strafprozessrecht, Rn. 10.

149 Einen ersten Überblick bietend *Schmitt* in: Meyer-Goßner/Schmitt, Einl. Rn. 55a, vgl. ausführlich § 5, B., I), 3).

150 BGHSt 31, 302, 309; BGHSt 38, 214, 220; BGHSt 51, 285, 290; *Fischer* in: KK-StPO, vor § 1 StPO, Rn. 3.

151 *Heger/Pohlreich*, Strafprozessrecht, Rn. 15; *Beulke/Swoboda*, Strafprozessrecht, Rn. 8.

152 *Beulke/Swoboda*, Strafprozessrecht, Rn. 11; FS-Spendel/*Ranft*, 719,724; vgl. auch insgesamt *Rieß*, JR 2006, 269, 270 f.

Hand der Strafverfolgungsbehörden gelegt. Ein Zusammenspiel aus dem Legalitätsprinzip, § 152 Abs. 2 StPO, und dem Amtsermittlungsgrundsatz, §§ 155 Abs. 2, 160 Abs. 2, 244 StPO, verschaffen dem Opfer somit die Gewissheit, dass der an ihm verübten Straftat nachgegangen und der durch den Täter geschaffenen Normkonflikt vor Gericht verhandelt wird. Ergänzt werden die in diesem Zusammenhang maßgeblichen Opferrechte auf Strafverfolgung durch die Möglichkeit des Klageerzwingungsverfahren nach §§ 172 ff. StPO.

Hinsichtlich der Erlangung und Verwertung belastender digitaler Beweismittel müssen, um den sich aus dem Rechtsstaatsprinzip, dem Grundgesetz, der Charta der Grundrechte der Europäischen Union (GRC) und der Konvention zum Schutz der Menschenrechte ergebenden Anforderungen zu genügen, die gleichen Verfahrensgrundrechte und -prinzipien wie für sonstige Beweismittel gelten. Besondere Bedeutung haben in diesem Kontext das Recht auf ein faires Verfahren, der Nemo-tenetur-Grundsatz, die Unschuldsvermutung sowie der Gesetzesvorbehalt, als Notwendigkeit für alle Eingriffe staatlicher Gewalt.[153]

II) Beschränkungen

Die gegenseitige Begrenzung dieser Ziele wird im Bereich strafverfolgungsbehördlicher Ermittlungen und der sich hieran anschließenden Verwertung am deutlichsten. Die strafprozessual forcierte Wahrheitsermittlung unterliegt durch die Rechtsstaatlichkeit gezogenen Grenzen. So sind im Laufe eines Strafverfahrens zahlreiche gesetzliche Legitimationen erforderlich, um für Zwecke der Strafverfolgung in die (Grund)Rechte der Bürger eingreifen zu dürfen. Darüber hinaus werden die staatlichen Eingriffsbefugnisse durch die Bedeutung der Grundrechte auf Seiten der Betroffenen begrenzt.[154]

1) Vorbehalt des Gesetzes

Zur Vermeidung uferloser und unbeschränkter Ermittlungen ist es erforderlich, dass die Exekutive für sämtliche Handlungen, die in Grundrechte des Betroffenen eingreifen, hierzu von der Legislative ermächtigt wurde.

153 *Warken*, NZWiSt 2017, 289, 291.
154 *Fischer* in: KK-StPO, vor § 1 StPO, Rn. 4.

Dadurch ist sichergestellt, dass das Maß zulässiger Eingriffe im Vorhinein – ohne Bezug zur durch die Maßnahme konkret betroffenen Person – festgelegt ist.[155] Die vom Gesetzgeber verabschiedeten Eingriffsbefugnisse zur Beschneidung der bürgerlichen Rechte müssen dabei hinreichend bestimmt sein und dadurch ihre Rechtsfolge für den Einzelnen vorhersehbar machen.[156] Dies bedeutet, dass der Betroffenen die Reichweite des Gesetzes mit einer hinreichenden Sicherheit einschätzen kann.[157] Besondere Anforderungen sind an den Gesetzesvorbehalt im Falle geheimer Überwachungsmaßnahmen zu stellen, die gerade im Vorfeld eines Strafprozesses von wesentlicher Bedeutung sind. Mangels Kenntnis des Betroffenen von der konkreten gegen ihn durchgeführten Überwachungsmaßnahme, ist es ihm gerade nicht möglich, die Einhaltung der gesetzlichen Vorschriften unmittelbar zu kontrollieren. Dies bedeutet, dass der gesetzliche Schutz umso höher ausfallen muss und ihm dabei insbesondere die Aufgabe zuteilwird, vor willkürlichen Eingriffen zu schützen.[158] Besondere Bedeutung erlangen in diesem Zusammenhang spezielle Anordnungsbefugnisse, die Notwendigkeit einer abschließend bestimmten Anlasstat, zeitliche Beschränkungen und die Speicherungs- und Löschungsvorschriften der erhobenen Daten.[159] In diesem Zusammenhang führen der technische Fortschritt und die damit einhergehende Veränderung der Lebenswelt zu Zweifelsfällen, in denen sich der Gesetzesanwender die Frage stellen muss, ob ein neuartiger Sachverhalt noch durch eine allgemein oder gar in einem anderen Kontext normierte Ermächtigungsgrundlage gedeckt sein kann. Exemplarisch sei an die vor wenigen Jahren aufgetretene Frage erinnert, inwiefern mittels der allgemein gefassten Ermittlungsgeneralklauseln eine ausreichende Rechtsgrundlage für die Nutzung der sozialen Medien wie Facebook, Instagram, oder Twitter zu Ermittlungszwecken vorhanden ist.[160] Ob eine neue technische Ermittlungsmöglichkeit unter die normierten Eingriffsbefugnisse subsumiert werden kann, ist zunächst eine Frage des Wortlauts, der die „neue Maßnahme“ umfassen muss. Eine Analogienbildung scheidet jedenfalls bei den strafprozessrechtlich grund-

155 Vgl. auch zur Entwicklung des Gesetzesvorbehalts *Rogall*, Informationseingriff und Gesetzesvorbehalt, S. 11 ff.
156 EGMR, NJW 2016, 2013, Rn. 120; EGMR, NJW 2011, 1333, Rn. 60.
157 *Gaede* in: MüKo-StPO, Art. 8 EMRK, Rn. 21.
158 EGMR, NJW 2011, 1333, Rn. 63; EGMR, NJW 2010, 213 Rn. 78.
159 *Gaede* in: MüKo-StPO, Art. 8 EMRK, Rn. 22.
160 *Zöller*, ZStW 2012, 411, 421; *Henrichs/Wilhelm*, Kriminalistik 2010, 30, 33.

rechtsintensiven Eingriffen aus.[161] Im Anschluss ist eine systematische und teleologische Auslegung der Norm vorzunehmen, in der ebenfalls zu berücksichtigen ist, ob der womöglich geänderte Charakter des neuartigen Zugriffs noch dem Willen des historischen Gesetzgebers entspricht.[162]

2) Verfahrensrechtliche Beschränkungen

a) Verdachtsgrad

Die Ermächtigung der Strafverfolgungsbehörden, mittels staatlicher Ressourcen in die Grundrechte der Bürger einzugreifen, setzt grds. voraus, dass die betreffende Person diese Maßnahme durch ihr vorheriges Verhalten „provoziert" hat. Das Erfordernis eines sog. Anfangsverdachts, für den nach kriminalistischer Erfahrung Anhaltspunkte vorliegen, die es als möglich erscheinen lassen, dass eine verfolgbare Straftat begangen wurde,[163] verhindert zum Schutz des Bürgers eine staatliche Strafverfolgung ohne sachlichen Grund. Wenngleich in der Ermittlungspraxis der Rückgriff auf bloße Vermutungen zur Begründung eines Anfangsverdachts nicht genügt,[164] führt der Umstand, dass den Ermittlungsbehörden bei der Beurteilung des Anfangsverdachts ein nicht unerheblicher Beurteilungsspielraum zukommt, dazu, dass die Schwelle zum Anfangsverdacht schnell überschritten sein kann.[165] Aufgrund dessen implementierte der Gesetzgeber bei eingriffsintensiven heimlichen Maßnahmen zusätzliche Schutzvorkehrungen, um die Begründungsanforderungen des einfachen Anfangsverdachts zu erhöhen (vgl. §§ 100a, 100b Abs. 1 Nr. 2, 3 StPO; § 100c Abs. 1 Nr. 2, 3, 4 StPO).

b) Straftatenkataloge

Ebenso werden die Ermittlungsbefugnisse und damit die Wahrheitsermittlung durch die Normierung bestimmter Anlassstraftaten beschränkt. Diese

---

161 *Kudlich*, GA 2011, 193, 195; *Valerius*, JR 2007, 275, 276; *Gusy*, StV 2002, 153, 156; a.A.: *Schmitt* in: Meyer-Goßner/Schmitt, Einl., Rn. 193.
162 Vgl. *Singelnstein/Putzer*, GA 2015, 564, 566.
163 BGH, NStZ 1994, 499, 500.
164 *Schmitt* in: Meyer-Goßner/Schmitt, § 152 StPO, Rn. 4.
165 BGH, NJW 1970, 1543, 1544; BGH, NStZ 1988, 510, 511; OLG München, NStZ 1985, 549, 550; *Gercke* in: HK-StPO, § 152 StPO, Rn. 11.

Straftatenkataloge bringen aufgrund ihrer beständigen Ausweitung in den letzten Jahren mit sich, dass nahezu nur noch Straftaten aus dem Bereich der leichten Kriminalität ausgenommen bleiben.[166] An einem übergeordneten System hinsichtlich der Aufnahme bestimmter Straftaten in die Straftatenkataloge mangelt es.[167]

c) Subsidiaritätsklauseln

Eine weitere Einschränkung sollen die Eingriffsbefugnisse durch die Vielzahl unterschiedlich formulierter Subsidiaritätsklausel erfahren.[168] Gemeinsames Ziel sämtlicher Subsidiaritätsklauseln ist es, die entsprechende Ermittlungsmaßnahme aufgrund ihrer Eingriffsintensität bestenfalls nur in dem Falle, in welchem weniger grundrechtsintensive Maßnahmen nicht erfolgsversprechend sind, zum Einsatz gelangen zu lassen. Nicht von der Hand zu weisen ist vor diesem Hintergrund jedoch der Einwand *Zöllers*, der darauf hinweist, dass es zu Erreichung dieses Zieles das Instrument der Subsidiaritätsklauseln nicht bedarf.[169] Schließlich erfordert bereits der Grundsatz der Verhältnismäßigkeit, der selbstredend für sämtliche Eingriffsbefugnisse gilt, dass stets das mildeste Mittel zum Einsatz kommen muss.[170] Würde der Gesetzgeber folglich auf explizite Subsidiaritätsklauseln verzichten, würde dies den Grundrechtsschutz nicht verringern.[171]

d) Richtervorbehalt

Der Richtervorbehalt soll geplante Maßnahmen bereits im Vorfeld einer präventiven richterlichen Rechtmäßigkeitskontrolle unterziehen.[172] Dadurch soll zum einen ausgeglichen werden, dass die Strafverfolgungsbehörden zum einen oftmals nicht die erforderliche Neutralität besitzen,

166 *Zöller*, ZStW 2012, 411, 421.
167 *Zöller*, StraFo 2008, 15, 19.
168 Vgl. in etwa §§ 100a, b Abs. 1 Nr. 3, 100c Abs. 1 Nr. 4, 110a Abs. 1 S. 3 StPO, 100h Abs. 1 S. 1, 163f Abs. 1 S. 2 StPO.
169 *Zöller*, ZStW 2012, 411, 421.
170 *Zöller*, ZStW 2012, 411, 421; GS-Meyer/*Rieß*, S. 367, 371; *Schroeder*, GA 2005, 73, 74; *Zöller*, StraFo 2008, 15, 20.
171 *Zöller*, ZStW 2012, 411, 428.
172 *Brüning*, ZIS 2006, 29, 29; *Schnarr*, NStZ 1991, 209, 210; *Hilger*, JR 1990, 485, 488.

die bei der Abwägung mit den Verfolgungsinteressen für die Berücksichtigung der Freiheitsinteressen des Betroffenen notwendig ist,[173] und zum anderen dem Umstand Rechnung getragen werden, dass dem Betroffenen im Falle heimlicher Maßnahmen nicht durch eine vorherige Anhörung Rechtsschutz gewährt werden kann[174]. Würde man diesen bereits im Vorfeld einer Maßnahme informieren, so würde dies den Erfolg einer Maßnahme vollkommen zunichtemachen. Gleichwohl kam eine empirische Studie der Universität Bielefeld zum ernüchternden Ergebnis, dass die Ermittlungsrichter ihrer Kontrollpflicht meist kaum nachkommen.[175] Häufig werden die von der Staatsanwaltschaft vorbereiteten Beschlussentwürfe wörtlich übernommen, ohne diese einer eingehenden rechtlichen Kontrollprüfung zuzuführen. Mögliche Ursachen hierfür können sowohl der allgemeine Personalmangel in der Justiz, ein daraus resultierender Zeitdruck, der Vorsprung von Fachwissen bei den Strafverfolgungsbehörden sowie lückenhafte Entscheidungsgrundlagen sein.[176]

3) Beweisverwertungsverbote

Neben dem Grundrechtseingriff im Rahmen des staatlichen Zugriffs folgt ein weiterer Grundrechtseingriff durch die prozessuale staatliche Beweisverwertung. Auch wenn die Erlaubnis zur staatliche Beweiserhebung auch die Nutzung im Strafverfahren erlaubt,[177] bringt der abermalige Grundrechtseingriff oder jedenfalls dessen Fortwirkung[178] mit sich, dass auch die Verwertung den Grundsätzen der Verhältnismäßigkeit genügen muss. Schließlich dient die Existenz eines Beweisverwertungsverbotes – analog zum Erfordernis des Gesetzesvorbehalts – dem Schutz des Betroffenen vor stetig weiter und tiefergehenden staatlichen Ermittlungsmaßnahmen. Erst die Existenz eines Beweisverwertungsverbotes ermöglicht im Zusammen-

173 *Amelung*, JZ 1987, 737, 741.
174 *Hilger*, JR 1990, 485, 485.
175 zur Studie *Backes/Gusy*, Telefonüberwachung, S. 44; *dies*, StV 2003, 249 ff.; im Übrigen auch *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation, S. 447; *Brüning*, Der Richtervorbehalt, S. 215.
176 *Zöller*, ZStW 2012, 411, 429; *Backes/Gusy*, StV 2003, 249, 250.
177 *Ernst*, Verarbeitung und Zweckbindung von Informationen, S. 182; *Rogall*, Informationseingriff und Gesetzesvorbehalt, S. 98 ff.
178 Vgl. *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, S. 143 ff.

spiel mit dem Erfordernis einer Ermittlungsbefugnis ein vollkommenes Schutzkonzept zugunsten des Bürgers. Ansonsten wäre der Betroffene auch solchen Eingriffen der Exekutive, die keine Legitimation der Legislative in sich tragen im Ergebnis schutzlos ausgeliefert. Gerade weil der Betroffene im kompletten Strafverfahren dem Staat mit all dessen Ermittlungsmöglichkeiten als „kleiner Mann" gegenübersteht, ist es für eine rechtsstaatlich anzuvisierende Waffengleichheit elementar, dass das Anerkennen von Beweisverboten verhindert, dass die Ungleichheit zwischen dem Staat als Ankläger und dem Betroffenen einseitig zu Lasten des Betroffenen kippt.[179]

a) Wahrung der Rechte des Einzelnen

In erster Linie liegt der Schutz der Beweisverbote sicherlich in dem Schutz der Individualrechte des Einzelnen.[180] Besonders deutlich wird dieser Schutzzweck bei den Beweisverboten, die den Kernbereich höchstpersönlicher Lebensgestaltung schützen. Zum Schutz der Menschenwürde und des allgemeinen Persönlichkeitsrechts soll verhindert werden, dass hochsensible Informationen im Strafprozess öffentlich gemacht werden. Zwar kann auch bei sämtlichen unselbstständigen Beweisverwertungsverboten, die durch die Beweiserhebung bereits eingetretene Rechtsverletzung nicht mehr rückgängig gemacht werden, was jedoch nicht gegen eine derartige Schutzfunktion spricht. Schließlich wird durch das Beweisverwertungsverbot die hoheitliche Verwertung des Beweismittels im Gerichtsverfahren verhindert, was seinerseits eine erneute Rechtsverletzung begründen würde und die vorliegende Rechtsverletzung perpetuieren und bestätigen würde.[181] Führt man sich zudem vor Augen, dass die Strafprozessordnung letztlich die Umsetzung der verfassungsrechtlich gewährleisteten Rechte des Einzelnen darstellt und bereits deshalb auch den Charakter der Grundrechte als Abwehrrechte zum Individualschutz in sich trägt, so kann die Wahrung der Rechte des Einzelnen als Beweisverbotszweck nicht geleugnet werden.[182] Ähnlich ist dies bei den selbstständigen Beweisverwertungs-

179 *Eder*, Beweisverbote, S. 49.
180 *Volk/Engländer*, GK-StPO, § 28, Rn. 7; *Peres*, Strafprozessuale Beweisverbote und Beweisverwertungsverbote, S. 35 f.; *Amelung*, NJW 1991, 2533, 2534; *Schröder*, Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung, S. 33; *Rogall*, ZStW 1979, 1, 21.
181 *Rogall*, ZStW 1979, 1, 20.
182 *Schwaben*, Die personelle Reichweite von Beweisverwertungsverboten, S. 28 f.

verboten, die gerade auf Grund des durch die Verwertung erfolgenden, nicht zu rechtfertigenden, Verstoßes gegen verfassungsrechtliche Individualrechtspositionen ein Beweisverbot begründen.

b) Schutz der Wahrheitsfindung

Dass Beweisverbote auch der Wahrheitserforschung dienlich sind, mag auf den ersten Blick verwundern. So schränkt das Verbot ein Beweismittel im Prozess zu nutzen, die Möglichkeiten der Wahrheitsermittlungen primär ein. Unberücksichtigt bliebe dabei allerdings, dass eine vollständige Wahrheitserforschung stets von der Qualität der ihr zugrunde liegenden Beweismitteln abhängig ist. So erscheint es denkbar, dass ein durch verbotene Vernehmungsmethoden zustande gekommenes Geständnis vermeintlich einen eindeutigen Beleg für die Strafbarkeit verschiedener Personen liefert. Dennoch kann die Wahrheit nur rechtssicher hervorgebracht werden, wenn sämtliche Beweismittel zur Wahrheitserforschung ausgeschlossen werden, an deren Richtigkeit (starke) Zweifel bestehen. Sicherlich pointiert verdeutlicht der Fall von unter Foltermethoden gewonnenen Geständnissen diese Problematik, da sodann der Gefolterte unter Umständen ausschließlich zur Beendigung der Folter die gegen ihn erhobenen Vorwürfe einräumen wird, ohne dass dies mit der Wahrheit übereinstimmen muss.[183] Zwar mag dies in solch extremen Ausnahmefällen durchaus zutreffend sein, gleichwohl kann der Schutz der Wahrheitsfindung nicht durchgehend zur Begründung eines Beweisverwertungsverbotes herangezogen werden. Nähert man sich dieser Frage vor dem Hintergrund des Grundsatzes der freien Beweiswürdigung als einer der zentralen Prozessmaximen, so erkennt man, dass die Strafprozessordnung die Würdigung eines Beweismittels und damit auch dessen Beweiswert ausschließlich dem Richter zuweist.[184] Ein gesetzliches Verbot hinsichtlich bestimmter Beweismittel zur Optimierung der Wahrheitserforschung stünde diesem Grundsatz entgegen. Insbesondere verfolgt die Strafprozessordnung weder den Ansatz, dass ein Beweisverwertungsverbot von der Richtigkeit oder Verlässlichkeit des Beweismittels abhänge noch den absoluten Ansatz, dass nur ein solches Ereignis der Wahrheit entspricht, das unter Beachtung

183 *Trüg*, StV 2010, 528, 531; *Volk/Engländer*, GK-StPO, § 28, Rn. 7; *Eder*, Beweisverbote, S. 52 f.; vgl. *ders*. S. 53 ff. zu den unterschiedlichen Definitionsansätzen zum Begriff der Wahrheit.

184 *Amelung*, NJW 1991, 2533, 2534.

sämtlicher (prozessualer) Vorschriften zu Tage getreten ist. Tatsächlich kann der Richter sogar gezwungen sein, seinem Urteil einen Sachverhalt zugrunde zu legen, der sich so tatsächlich nicht zugetragen hat, da beispielsweise ein Geständnis des Zeugen aufgrund evidenter Verfahrensverstöße nicht verwertet werden darf.[185] In diesem Fall wird offensichtlich, dass ein Beweisverwertungsverbot das Ziel der Wahrheitsfindung konterkarieren kann und sodann tatsächlich einzig dem Schutz der Rechte des Betroffenen dient.

c) Aufrechterhaltung der hoheitlichen Straflegitimation

Nicht unmittelbar einleuchtend erscheint womöglich, dass das Anerkennen von Beweisverwertungsverboten die hoheitliche Straflegitimation bewahren soll.[186] Dies wird gerade dann deutlich, wenn Straftaten im Raum stehen, die durch die breite Öffentlichkeit auf sittlich unterster Stufe angesiedelt werden. Zu denken ist hier beispielsweise an Missbrauchsfälle. In diesen Fällen muss bei Betrachtung der vorherrschenden Meinung in der Bevölkerung davon ausgegangen werden, dass in einem solchen Zusammenhang das Anerkennen eines Beweisverbotes auf blankes Entsetzen stoßen und die durch ein Beweisverbot verfolgte Aufrechterhaltung der hoheitlichen Straflegitimation wohl gar in ihr Gegenteil verkehrt würde. Nähert man sich dieser Fragestellung jedoch weniger von einer emotionalen Seite, sondern vielmehr vom Blickwinkel der theoretischen Legitimation des Strafens, so muss beachtet werden, dass mit eben dieser vom Volke auf den Staat übertragenen Legitimation des Strafens die Verpflichtung einherkommt, im Sinne des gemeinsamen Rechts zu handeln. Ansonsten kann eben diese Legitimation verloren gehen, wenn bei deren Durchsetzung selbst Recht gebrochen wird.[187] Dies erkannte auch der BGH und betonte, dass das ungesetzliche Strafen dem Vertrauen in die Rechtsstaatlichkeit der Strafrechtspflege mehr schadet, als es die Gerechtigkeit befriedigt, wenn ein Täter zur Rechenschaft gezogen wird.[188] Ob die Glaubwürdigkeit einer staatlichen Sanktion erst dann zu leiden beginnt, wenn der Staat die der Sanktion zugrunde liegenden Beweismittel unter einem Verstoß gegen elementare Rechte wie die Menschenwürde beschafft

185 *Brandis*, Beweisverbote als Belastungsverbote, S. 38 f.
186 *Eisenberg*, Beweisrecht der StPO, Rn. 363; Mosbacher, NJW 2007, 3686, 3688.
187 *Dencker*, Verwertungsverbote im Strafprozess, S. 59 ff.
188 BGHSt 18, 274, 278.

oder bereits, wenn der Staat unter Verstoß gegen einfach geltendes (Straf-) Recht Informationen erlangt und sich so in eine Art Selbstwiderspruch verwickelt, bleibt unklar.[189] Ausgehend davon, dass sich die Legitimation des staatlichen Strafanspruchs wesentlich aus der Aufrechterhaltung der gesellschaftlichen Ordnung ergibt, folgt jedenfalls, insbesondere aus generalpräventiven Aspekten, dass das Vertrauen in die Strafrechtspflege im Allgemeinen nur bei einem rechtmäßigem Verfahren gewonnen werden kann.[190] Im Grundsatz ist daher davon auszugehen, dass, wenn der Staat auf Grundlage rechtswidrig erlangter Beweise den Beschuldigten einer Strafe zuführt, dies auf Dauer der staatlichen Legitimation schaden würde. Zwar kann nicht widerlegt werden, dass bei beschriebenen Straftaten die Akzeptanz des staatlichen Strafens auch bei einer rechtswidrigen Vorgehensweise bei einem Großteil der Bevölkerung nicht schwinden würde, was jedoch nichts an der Tatsache zu ändern vermag, dass ein Strafverfahren rechtsstaatlichen Grundsätzen genügen muss. In anderen Zusammenhängen ist dieser Prämisse wohl auch das öffentliche Meinungsbild einhellig zugeneigt, beispielsweise dann, wenn der Blick auf das staatliche Vorgehen in totalitär ausgerichtete Staaten wandert, in denen beispielsweise ein willkürliches Vorgehen der Behörden prägend für die Ermittlungsarbeit ist.

d) Disziplinierungsgedanke

Der Disziplinierungsgedanke eines Beweisverwertungsverbotes stellt eine Konsequenz des amerikanischen Strafprozesses dar, der mit der Anklagebehörde und dem Angeklagten als Parteienprozess ausgestaltet ist.[191] Im Unterschied zum deutschen Strafprozess wird die Wahrheit dort nicht von Amts wegen erforscht, sondern die Ermittlungen werden maßgeblich durch die Parteien vorangetrieben, die ihr Ergebnis sodann den Geschworenen präsentieren und versuchen die Beweisführung der Gegenseite zu widerlegen. Überschreiten dabei die Ankläger die gesetzlichen Leitlinien, so wird ihr das so gewonnene Beweismittel (durch den Richter gewissermaßen als Schiedsrichter) genommen und sie muss zum Obsiegen der

189 *Amelung*, StraFo 1999, 181, 182.
190 *Eder*, Beweisverbote, S. 63; *Dencker*, Verwertungsverbote im Strafprozess, S. 59 ff.
191 *Paulsen*, ZStW 1965, 637, 656; *Schröder*, Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung, S. 28.

Auseinandersetzung auf andere Beweismittel zurückgreifen.[192] Dies entspricht auch den Grundsätzen des deutschen Parteienprozesses im Zivilrecht, wie die Präklusionsvorschrift des § 296 ZPO zeigt.[193] Im deutschen Strafprozess als Offizialverfahren sind allerdings das Gericht und die Ermittlungsbehörden nach §§ 160 Abs. 2, 244 Abs. 2 StPO beauftragt die Wahrheit zu ermitteln. Selbst die Staatsanwaltschaft als Ankläger stellt dabei nicht den Gegner des Angeklagten dar, mit dem dieser um den Sieg vor Gericht ringt. Nichtsdestotrotz wurde vor allem in der älteren Literatur die Notwendigkeit der Beweisverbote im deutschen Strafprozess teilweise mit der Disziplinierung der Strafverfolgungsbehörden begründet.[194] Vor dem Hintergrund, dass auf Grundlage eines rechtsbrüchigen Verhaltens keine gerichtlich belastbaren Ermittlungsergebnisse erzielt werden dürfen, sollte ein solches Verhalten für die Strafverfolgungsbehörden als nicht lohnenswert erscheinen. Den Beweisverwertungsverboten sollte so gleichsam ein generalpräventiver Aspekt künftigen Rechtsverletzungen entgegenzuwirken zu Teil werden.[195] Dieser Gedanke kann jedoch bei selbstständigen Beweisverwertungsverboten, bei denen es gerade an einem gesetzeswidrigen Vorgehen der Strafverfolgungsbehörden fehlt, ein Beweisverwertungsverbot nicht begründen.[196] Zudem ist es in der Tat so, dass, wenn einzig die Disziplinierung der Beamten die Notwendigkeit eines Beweisverbotes begründen würde, diese Disziplinierung auch durch entsprechende Disziplinarmaßnahmen bis hin zur Entlassung aus dem Dienst erreichbar wäre.[197] Die Begründung eines Beweisverwertungsverbots aufgrund eines Disziplinierungsgedankens kann ferner auch deshalb nicht überzeugen, da die Strafverfolgungsbehörden in Fällen, in denen die Beweisbarkeit der Täterschaft durch ein ordnungsgemäßes Vorgehen ohnehin nicht zu erbringen wäre, keinen Grund hätten, sich vor der Disziplinierung mittels eines Beweisverwertungsverbotes zu fürchten. Gerade dann, wenn die Beweislage aussichtslos ist und die Ermittlungsbehörden

192 *Brandis*, Beweisverbote als Belastungsverbote, S. 45.
193 *Schröder*, Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung, S. 29.
194 *Osmer*, Umfang des Beweisverwertungsverbotes, S. 46; *Spendel*, NJW 1966, 1102, 1108; die Disziplinierung als Hintergrundfunktion einordnend *Nüse*, JR 1966, 281, 284 f.; *Fezer*, JR 1992, 385, 387; *Strate/Ventzke*, StV 1986, 30; *Rogall*, ZStW 1979, 1, 15; ablehnend *Dencker*, Verwertungsverbote im Strafprozess, S. 54; FS-Spendel/*Ranft*, 719,725.
195 *Grünwald*, JZ 1966, 489, 499.
196 *Küpper*, JZ 1990, 416, 417.
197 *Jäger*, Beweisverwertung und Beweisverwertungsverbote, S. 70.

sprichwörtlich nichts zu verlieren haben, kann ein Verwertungsverbot kaum disziplinierend wirken.[198] Nicht zuletzt ist zu beachten, dass der Disziplinierungsgedanke ausnahmslos jeden Verfahrensverstoß mit einem Beweisverwertungsverbot belegen müsste, was in dieser Rigorosität nicht erstrebenswert ist. Gleichwohl ist nicht von der Hand zu weisen, dass ein aufgrund eines Verwertungsverbot eintretender Beweismittelverlust in vielen Fällen geeignet sein wird, die Justizorgane zur exakten Beachtung der einschlägigen Vorschriften zu animieren.[199] Insofern können Beweisverbote im deutschen Strafprozessrecht zwar nicht tragend auf dem Disziplinierungsgedanken aufbauen, dennoch kann einer mittelbaren Disziplinierungswirkung etwaiger Beweisverbote nicht gänzlich widersprochen werden.

B. Elektronische Daten im Strafprozess

Die fortschreitende Digitalisierung, mithin das Vordringen der elektronischen Datenverarbeitung in den Alltag und die Vielzahl unterschiedlicher Datenquellen, lässt auch die Existenz digitaler Daten stetig zunehmen. Dabei hat sich der Begriff „Big Data" etabliert, der zwar keiner genauen Definition zuzuführen ist, jedoch als das Phänomen der massenhaften Datenverfügbarkeit verstanden wird.[200] Nur beispielshaft sei an die heute überwiegend digital ablaufende schriftliche Korrespondenz, elektronische Fotografie- und Videoaufnahmen, die Interaktion in digitalen sozialen Medien, online-Banking, Navigationssysteme im Auto, bargeldloses Bezahlen, oder kommunizierende Fitnessbänder oder Multifunktionsuhren erinnert. Erst kürzlich stand mit der Videoüberwachung öffentlicher Plätze eine Maßnahme, die zudem große Mengen entsprechenden Bildmaterials erzeugt im Zentrum der politischen Diskussion. Nicht zuletzt führt die im Rahmen dieser Arbeit relevante zunehmende Vernetzung mit internetfähigen Geräten unmittelbar zur Entstehung großer Datenmengen.[201] Für

198 *Jäger*, Beweisverwertung und Beweisverwertungsverbote, S. 70.

199 *Rogall*, ZStW 1979, 1, 15, der zutreffend ausführt, dass derjenige, der die Sinnlosigkeit seines Verhaltens vor Augen hat, eben von diesem sinnlosen Verhalten Abstand nehmen wird; BGH, NStZ-RR 2021, 142, 143, der im Zusammenhang mit dem absoluten unselbstständigen Beweisverwertungsverbot aus § 136a Abs. 3 S. 2 StPO erstmals von einer Sanktionsfunktion zu Lasten verbotswidrig handelnder Strafverfolgungsbehörden spricht.

200 *Warken*, NZWiSt 2017, 329, 332.

201 Vgl. mit weiteren Beispielen *Warken*, NZWiSt 2017, 329, 332 f.

die Ermittlungsbehörden bedeutet dies neue rechtliche sowie technische Probleme. So stellt die Erlangung umfangreicher Datensätze, bereits deshalb eine nicht zu unterschätzende Herausforderung dar, da die Analyse dieser Daten einen erheblichen Zeitbedarf bedarf und große Personalkapazitäten benötigt. Aus rechtlicher Sicht stehen insbesondere die staatlichen Möglichkeiten auf diese digitalen Daten zuzugreifen und gleichsam die Frage nach einem effektiven Datenschutz und dem Schutz der Persönlichkeitsrechte der Betroffenen im Vordergrund. Mit der Erwartung, dass solche digitale Daten das Strafverfahren in Zukunft noch stärker prägen als dies ohnehin bereits der Fall ist,[202] muss auch der sich damit intensivierenden Gefahr für das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in Form des Rechts auf informationelle Selbstbestimmung, der Integrität von informationstechnischen Systemen oder dem Recht am eigenen Bild im Gleichschritt Rechnung getragen werden.[203]

I) Einbringung elektronischer Daten in den Strafprozess

Es bleibt zu fragen, wie die Einbringung elektronischer Daten im Strafprozess im Rahmen des numerus clausus der durch die Strafprozessordnung anerkannten Beweismittel möglich ist. Der deutsche Strafprozess ist gezeichnet durch das Strengbeweisverfahren.[204] Mithin dürfen für diejenigen Tatsachen und Erfahrungssätze, auf denen das tatrichterliche Urteil (Schuld- und Strafausspruch) beruht, nur die in der Strafprozessordnung genannten Beweismittel in Betracht kommen.[205] Der dortigen Aufzählung von Zeugen, Sachverständigen, Augenschein, Urkunden sowie in gewissem Rahmen der Beschuldigtenaussage[206], sind elektronische Daten als zugelassenes Beweismittel nicht zu entnehmen. Anknüpfend an das Charakteristikum elektronischer Daten in Form deren fehlender Körperlichkeit, findet sich eine Ähnlichkeit zu den anerkannten Beweismitteln nicht bereits auf den ersten Blick. Eine Betrachtung anderer Prozessordnungen zeigt jedoch, dass der Gesetzgeber die Relevanz elektronischer Daten im Prozess durchaus erkannt hat. In die Zivilprozessordnung erhielten elek-

202 *Momsen*, Cybercrime und Cyberinvestigations, 67, 71.
203 *Fährmann*, MMR 2020, 228.
204 BGH, NJW 1961, 1486, 1487; *Trüg/Habetha* in: MüKo-StPO, § 244 StPO, Rn. 35 m.w.N.
205 *Krehl* in: KK-StPO, § 244 StPO, Rn. 8; *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 2; *Eisenberg*, Beweisrecht der StPO, Rn. 35.
206 *Schmitt* in: Meyer-Goßner/Schmitt, Einl., Rn. 49.

tronische Dokumente gleich an mehreren Stellen Einzug: Während die §§ 130a, 130b ZPO regeln, wie Schriftsätze von den Prozessbeteiligten wirksam in elektronischer Form eingebracht werden können, bestimmen die §§ 298, 298a ZPO den Umgang und die Möglichkeit elektronischer Aktenführung. Beweisrechtlich entscheidend ist § 371 Abs. 1 ZPO. Gem. § 371 Abs. 1 S. 2 ZPO erfolgt die Beweisführung bei Vorliegen elektronischer Dokumente durch Augenschein. Gleiches gilt durch den Verweis in § 98 VwGO auf die Vorschriften der Zivilprozessordnung auch im verwaltungsgerichtlichen Verfahren. In der Strafprozessordnung sucht man – mit Ausnahme des § 41a StPO, der schriftliche Erklärungen, sofern diese mit einer elektronischen Signatur versehen sind, auch in elektronischer Form zulässt – nach entsprechenden Regelungen vergebens. Trotz der erheblichen Bedeutung digitaler Daten für das Strafverfahren findet sich in der Strafprozessordnung weder ein konkretisierter Datenbegriff noch detaillierte Vorschriften für das Einbringen eines solchen Beweises in den Prozess. Zurückzuführen ist dies wohl auf die Entstehungsgeschichte der Strafprozessordnung, zu deren Gründungszeit Ende des 19. Jahrhunderts es nicht denkbar war, dass elektronische Daten Teil einer strafrechtlichen Beweiserhebung sein würden.[207] Ob dies angesichts der stetig zunehmenden Digitalisierung, von der sich auch der Strafprozess nicht freizeichnen kann, heute noch sachgemäß erscheint, darf bezweifelt werden.

1. Zeugenbeweis

Der in den §§ 48 bis 71 der StPO geregelte Zeugenbeweis, ist maßgeblich in § 69 StPO normiert. Der mündliche zu vernehmende Zeuge, berichtet dem Gericht von eigenen Wahrnehmungen, nicht aber von Erfahrung oder Rechtsmeinungen.[208] Im Zuge der Vernehmung obliegt es der richterlichen Beweiswürdigung, die Glaubhaftigkeit der Zeugenaussage zu überprüfen. Im Zusammenspiel mit elektronischen Beweismitteln ist es dabei beispielsweise möglich, dass Ermittler als sachverständiger Zeuge vernommen werden, die darüber berichten, wie sie bei den Ermittlungen Kenntnisse der forensischen Informatik angewandt haben. Im Übrigen können die Ermittlungsbeamten darüber aussagen, wie sie das aufgezeichnete Gespräch selbst erlebt haben oder könnten darüber befragt werden, was sie möglicherweise im Zuge der Beschlagnahme eines Speichergeräts

207 *Trüg*, StV 2016, 343.
208 *Heinson*, IT-Forensik, S. 108.

wahrgenommen haben. Die Ermittler können etwa gebeten werden, Ermittlungsergebnisse zu erläutern oder können zusätzlich zum Ablauf der Ermittlungen, den eingesetzten (technischen) Mitteln oder dem Aussagegehalt der elektronischen Dateien befragt werden.[209]

2. Sachverständigenbeweis

Der vom Gericht oder der Staatsanwaltschaft beauftragte Sachverständige gibt Auskunft über Tatsachen oder Erfahrungssätze, die für bestimmte Beweisfragen benötigt werden oder beurteilt einen bestimmten Sachverhalt auf Grundlage seiner besonderen Fachkunde.[210] Ob sich das Gericht eines Sachverständigen bedient oder auf seine eigene Sachkunde vertraut, steht grundsätzlich in dessen Ermessen. Bestehen beim Gericht jedoch Zweifel hinsichtlich der eigenen Sachkenntnis oder liegt der Entscheidungsfindung ein anspruchsvoller technischer Vorgang zu Grunde, so ist das gerichtliche Ermessen regelmäßig derart reduziert, dass dieses auf die besondere Sachkunde eines Sachverständigen zurückgreifen muss.[211] Auch im Bereich digitaler Daten kann es erforderlich sein, dass ein Sachverständiger zu möglichen Fragen der Verfahrensbeteiligten ein Gutachten fertigt, § 75 StPO. So können die gefundenen Daten begutachtet oder die Untersuchungsergebnisse anhand der Regeln der Fachdisziplin (auf ihre Authentizität) geprüft werden. Dies kann dadurch geschehen, dass der Sachverständige die Art und Weise der Datenerhebung begutachtet und damit die Technik und das Verfahren hinsichtlich der Sicherung und Analyse der erhobenen Daten verifiziert.[212] Diese Begutachtung ermöglicht dem Gericht, den Beweiswert der vorliegenden Daten besser einschätzen zu können.

3. Urkundenbeweis

Die Einbringung durch Urkundenbeweis nach § 249 StPO erfolgt durch Verlesen eines Schriftstücks, wodurch über den verkörperten Gedankeninhalt Beweis erhoben wird. Voraussetzung hierfür ist, dass die in der

209 *Heinson*, IT-Forensik, S. 108.
210 *Heinson*, IT-Forensik, S. 109.
211 BGH, MMR 2007, 178, 179.
212 *Heinson*, IT-Forensik, S. 122.

Urkunde verkörperte Gedankenerklärung aus sich heraus verständlich und durch einfaches Verlesen in der Hauptverhandlung allen Beteiligten zu verstehen gegeben werden kann.[213] Hinzuweisen ist an dieser Stelle auf § 256 Abs. 1 Nr. 1 StPO, der beispielsweise die Möglichkeit eröffnet, Gutachten von vereidigten Sachverständigen zu verlesen. Insofern durchbricht diese Art des Urkundenbeweises den Unmittelbarkeitsgrundsatz des § 250 StPO. Dies vereinfacht das Verfahren, da die umfangreiche Analyse elektronischer Daten regelmäßig als schriftliches Gutachten wiedergegeben werden kann.[214] Gleichwohl wird teilweise angenommen, dass dieses Vorgehen, mithin das Anfertigen und Verlesen eines schriftlichen Vermerkes über den Inhalt die Inaugenscheinnahme einer Videoaufzeichnung oder Tonaufnahme nicht ersetzen kann. Der Unmittelbarkeitsgrundsatz und damit die Prämisse sich des sachnächsten Beweismittels zu bedienen, wird durch § 256 StPO nicht obsolet.[215] Dem ist der BGH in gewisser Weise entgegengetreten. Sofern die durch Tonaufnahmen und digitale Aufzeichnungen gewonnenen Informationen in einer Niederschrift festgehalten werden, können diese auch mittels Verlesung durch Urkundenbeweis in den Prozess eingebracht werden.[216] Der BGH stellte dahingehend fest, dass selbst wenn Tonbandaufzeichnungen Gegenstand des Augenscheinbeweises sind, damit nicht feststeht, dass ihr Inhalt allein in dieser Form für die Überzeugungsbildung des Gerichts benutzt werden dürfe.[217] Die Schlussfolgerung, dass dem Beweis zugängliche Tatsachen nur in der Gestalt verwendet werden dürfen, in der sie sich ursprünglich in der Außenwelt manifestieren und jede Transformierung von Beweismitteln unzulässig sei, ist der Rechtsordnung fremd.[218] Das Gesetz selbst sehe schließlich in den §§ 251 ff. StPO die Möglichkeiten der Ersetzung des Zeugenbeweises durch den Urkundenbeweis vor.[219]

213 *Mosbacher* in: LR-StPO, § 249 StPO, Rn. 7.
214 *Heinson*, IT-Forensik, S. 112.
215 *Heinson*, IT-Forensik, S. 112; OLG Düsseldorf, NStZ 2008, 358, dessen Urteil sich jedoch auf die Verlesung des Vermerks der schriftliche Erklärung eines Zeugen bezog, der berichtete was sein Augenschein ergab.
216 BGHSt 27, 135, 136.
217 BGHSt 27, 135, 136.
218 BGHSt 27, 135, 136.
219 BGHSt 27, 135, 137.

4. Inaugenscheinnahme

Die richterliche Inaugenscheinnahme nach § 86 StPO erfolgt durch Sinneswahrnehmungen jeder Art, daher durch Hören, Sehen, Riechen, Fühlen oder Schmecken.[220] Die Inaugenscheinnahme soll dabei Aufschluss über die Existenz oder Beschaffenheit einer Sache, eines Vorgangs oder einer Verhaltensweise geben.[221] Der Bundesgerichtshof ordnete die klassische Tonbandaufzeichnung zwar als Objekt der Inaugenscheinnahme ein, führte aber gleichfalls aus, dass daraus kein Gebot abzuleiten sei eine Tonbandaufzeichnung ausschließlich durch Augenschein in die Hauptverhandlung einzuführen.[222]

II) Einordnung der Audioaufzeichnungen eines Sprachassistenten

Es bleibt daher zu fragen, in welcher Form Audioaufzeichnungen eines Sprachassistenten in den Strafprozess einzubringen sind. Dies ist unter anderem vor dem Hintergrund relevant, dass im Falle einer Einbringung durch Inaugenscheinnahme die besonderen prozessualen Vorgaben über den Urkundenbeweis in Form der §§ 249 ff. StPO nicht anwendbar wären. Daran anknüpfend erhob eine ältere Literaturauffassung rechtsstaatliche Bedenken, sofern die Audioaufzeichnungen durch eine Beweisführung mittels Inaugenscheinnahme in den Strafprozess eingebracht würden, da mangels Anwendbarkeit der Beweisverbote der §§ 250 ff. StPO kein hinreichender Schutz in Anbetracht der hohen Missbrauchsgefahr (Echtheit der Aufnahme) bestünde.[223] Daher sollen Audioaufzeichnungen nur dann im Sinne des Augenscheins eingebracht werden dürfen, wenn die Unversehrtheit der Aufnahme festgestellt oder ein Stimmenabgleich durchgeführt werden soll. In allen anderen Fällen müssten ansonsten die §§ 250 ff. StPO analog auch auf den Augenscheinbeweis angewandt werden. Dies hätte zur Folge, dass das Tonband seiner selbstständigen Beweisfunktion weitgehend beraubt wäre, da die Beweisverbote der §§ 250 ff. StPO in fast allen Fällen die persönliche Vernehmung der zu hörenden Person erfordern

220 So bereits BGHSt 18, 51,53; *Schmitt* in: Meyer-Goßner/Schmitt, § 86 StPO, Rn. 1; *Feldmann*, NJW 1958, 1166, 1168.
221 *Eisenberg*, Beweisrecht der StPO, Rn. 2220.
222 BGHSt 27, 135, 136.
223 *Dallinger*, MDR 1956, 143, 146.

würden.[224] Dies überzeugt nicht. Der möglicherweise verminderte Wahrheitsgehalt eines Beweismittels kann nicht über dessen Zulässigkeit entscheiden bzw. das Beweismittel faktisch entwerten. Insofern ist *Eisenberg* zuzustimmen, dass schließlich auch derjenige als Zeuge und damit als Beweismittel in Betracht kommt, der als unglaubwürdig gilt.[225] Ferner ist zu beachten, dass diese veraltete Literaturansicht auf dem Verständnis einer Tonaufnahme als im Ermittlungsverfahren gefertigte Vernehmungsaufnahme zur späteren Verwertbarkeit fußt.[226] Daher ist diese Literaturansicht schon gar nicht auf den Fall der durch Sprachassistenten aufgenommen Aufzeichnungen übertragbar. Schließlich wird es sich bei den dort aufgezeichneten Aufnahmen kaum um Vernehmungssituationen handeln. Daher wären die den Unmittelbarkeitsgrundsatz aus § 250 StPO schützenden §§ 251 ff. StPO in solchen Situationen nach Sinn und Zweck ohnehin nicht anwendbar, da der Grundsatz der Unmittelbarkeit nur verbietet, dass eine Vernehmung durch die Verlesung eines Protokolls ersetzt wird.

Die Einbringung durch Inaugenscheinnahme würde darüber hinaus auch das Selbstleseverfahren, § 249 Abs. 2 S. 1 StPO ausschließen und wäre ferner dem Ablehnungsgrund des § 244 Abs. 5 S. 1 StPO unterworfen.[227] Gerade der Ausschluss des Selbstleseverfahrens würde eine adäquate Prozessvorbereitung der Parteien in solchen Fällen verhindern, in denen Audioaufzeichnungen über mehrere Stunden vorliegen. Zudem kennt die Strafprozessordnung selbst keinen Grundsatz, aus dem abzuleiten wäre, dass das Gericht das jeweils sachnächste Beweismittel (Audioaufzeichnung) anstelle möglicher Surrogate (Verschriftlichung des Inhalts der Audioaufzeichnung) zu verwenden hat.[228] Aus der StPO lässt sich daher kein Vorrang der Inaugenscheinnahme in Form einer auditiven Wahrnehmung durch das Abhören der Sprachaufzeichnung gegenüber dem Urkundenbeweis herleiten. Systematisch stellt die Inaugenscheinnahme vielmehr eine Auffangfunktion gegenüber dem Urkundenbeweis dar. Auch beim Urkundenbeweis kommt es in Folge des Vorlesens zu einer sinnlichen Wahrnehmung, sodass der Urkundenbeweis letztlich einen Spezialfall des Inaugenscheinbeweises darstellt.[229] Für eine Art „Auffangtatbestand" der Inaugenscheinnahme sprechen auch die verminderten Anforderungen an die

224 *Schmitt*, JuS 1967, 19, 21; *Kohlhass*, NJW 1957, 81, 83.
225 *Eisenberg*, Beweisrecht der StPO, Rn. 2292.
226 *Feldmann*, NJW 1958, 1166, 1168.
227 *Trüg*, StV 2016, 343, 344.
228 *Eisenberg*, Beweisrecht der StPO, Rn. 2223.
229 *Trüg*, StV 2016, 343, 344; *Schmitt* in: Meyer-Goßner/Schmitt, § 86 StPO, Rn. 1; *Krause* in: LR-StPO, § 86 StPO, Rn. 1.

Ablehnung eines Beweisantrages nach § 244 Abs. 5 S. 1 StPO, wonach der Antrag auf Inaugenscheinnahme nach dem Ermessen des Gerichts bereits dann abgelehnt werden kann, sofern er zur Erforschung der Wahrheit für nicht erforderlich gehalten wird. Dem Urkundenbeweis folgt neben dem Vorteil eines möglichen Selbstleseverfahren auch der, dass durch die technische Aufarbeitung vermieden wird, dass Audioaufzeichnungen aufgrund schlechterer Qualität, über die dem Gericht zur Verfügung stehenden Medien in der Hauptversammlung nur in unzureichender Qualität vorgespielt werden können. Problematisch dabei ist allerdings, dass durch ein bloßes Verlesen der Protokolle bestritten werden könnte, dass die aufgezeichnete Sprachnachricht tatsächlich von der angeklagten Person stammt. Sodann müsste im Wege eines Sachverständigengutachtens oder letztlich doch im Rahmen einer Inaugenscheinnahme die Zuordnung der Stimmen der Audioaufzeichnung zum Angeklagten erfolgen. Hinzu kommt, dass durch eine Niederschrift der Tonaufzeichnung die emotionale Situation des Angeklagten zum Aufnahmezeitpunkt aufgrund der nicht wahrnehmbaren Stimmlage oder Laustärke nicht berücksichtigt werden könnte. Zur Einordnung digitaler Sprachaufzeichnungen kann schließlich ein Vergleich mit in den Strafprozess einzubringenden elektronischen Schriftstücken dienen. Bei elektronischen Schriftstücken wird der Gedankeninhalt, der in den elektronischen Daten bereits vorhandenen schriftlichen Texte, zur Einbringung in den Prozess visualisiert. Das Verlesen ist Schriftstücken – gleich ob elektronisch oder analog – immanent. Daher ist bei elektronischen Schriftstücken im Gesamten eine Beweiseinbringung durch Urkundenbeweis vorzunehmen.[230] Bei elektronischen Audiodateien liegt die für eine Urkunde notwendige Verschriftlichung und damit Verlesbarkeit in den bereits existenten Daten allerdings gerade nicht vor. Vielmehr ist eine Audioaufzeichnung primär der auditiven Wahrnehmung durch Inaugenscheinnahme zuzuordnen.[231] Dies bringt insbesondere den Vorteil mit sich, dass der Zuhörende durch das Abspielen der Audioaufzeichnung exakt denjenigen Geschehensablauf – inklusive Emotionen, Lautstärke und ähnlichen subjektiven Empfindungen – zu hören bekommt, wie er sich tatsächlich zugetragen hat.[232] Die Aufzeichnung ermöglicht es dem

230 Vgl. zum Gesamten hinsichtlich elektronischer Schriftstücke: *Trüg*, StV 2016, 343, 344; in diesem Zusammenhang ordnete der BGH nun erstmals die Verlesung des Ausdruckes einer ansonsten nur digital vorliegenden E-Mail als präsentes Beweismittel i.S.d. § 245 StPO ein, vgl. BGH, StV 2021, 780, 781; so bereits zuvor *Trüg*, StV 2016, 343, 345.

231 So auch zu Film- und Videoaufnahmen *Metz*, NStZ 2020, 9.

232 *Wenskat*, Der richterliche Augenschein, S. 33; *Metz*, NStZ 2020, 9, 9.

Richter, sich in die Situation zu versetzen als wäre er selbst bei dem beweisgegenständlichen Gespräch vor Ort gewesen, was ihm eine Tatsachenfeststellung durch eine eigene akustische Wahrnehmung ermöglicht, ohne dass andere Personen wie Zeugen und Sachverständige zwischengeschaltet wären.[233] Somit sind Übermittlungsfehler oder dem Zeugenbeweis potenziell anhaftende Fehlerquellen bezüglich des Erinnerns und Wiedergebens des Beobachteten ausgeschlossen. Die Audioaufzeichnung stellt schließlich eine objektiv und nüchterne Wiedergabe des Geschehens dar.[234] Insofern kann die beweisrechtliche Sicherheit des Sachbeweises in Form der abgespielten Audioaufzeichnungen einen möglicherweise fehleranfälligeren Personalbeweis überwiegen. Es ist im Einzelfall unter Berücksichtigung der hier genannten Argumente jedoch dem tatrichterlichen Ermessen zu überlassen, welcher zur Verfügung stehender Beweise sich dieser bedienen will.[235] Sofern eine Niederschrift der Audioaufzeichnung verlesen wird, ist erforderlich, dass sich das Gericht von deren Korrektheit überzeugt. Hiervon darf ausgegangen werden, solange keine Zweifel an der Richtigkeit und Vollständigkeit der Verschriftlichung bestehen, da diese beispielsweise durch als allgemein zuverlässig geltende Personen angefertigt wurden. In Zweifelsfällen ist die Tonaufnahme andernfalls in Augenschein zu nehmen.[236]

III) Beweiswert

Zur Vornahme der richterlichen Beweiswürdigung elektronischer Daten im Allgemeinen, muss zunächst das Hindernis überwunden werden, dass sich computergespeicherte Daten im Wege der Inaugenscheinnahme nicht unmittelbar wahrnehmen lassen. Es bedarf einer Aufbereitung mittels Ausdruckens, Abspielens oder einer Transkription.[237] Letztlich werde das Beweismittel erst durch diesen Zwischenschritt „gerichtstauglich". *Momsen* spricht in diesem Zusammenhang gar von „der Herstellung des Beweismittels"[238]. Diese Formulierung ist sicherlich überspitzt formuliert, doch

233 *Metz*, NStZ 2020, 9, 9.
234 *Metz*, NStZ 2020, 9, 9.
235 BGHSt 27, 135, 136.
236 *Kreicker* in: MüKo-StPO, § 249 StPO, Rn. 22; zu einer Inaugenscheinnahme der aufgezeichneten Audioaufzeichnungen kam es in, LG Regensburg, Urteil vom 16. Dezember 2020 – Ks 103 Js 28875/19.
237 *Heinson*, IT-Forensik, S. 113.
238 FS-Beulke/*Momsen*, 871, 877.

gleichwohl offenbart sie die Problematik, die mit der Notwendigkeit solcher Zwischenschritte einhergeht. Die notwendige Aufbereitung kann den Beweiswert der vorliegenden Daten beinträchtigen. Beispielsweise kann nicht garantiert werden, dass die Dateien inhaltsgleich mit der Originaldatei wiedergegeben werden. Neben möglicherweise technischen Fehlern im Rahmen der Konvertierung, offenbaren elektronische Dateien auch eine erhöhte Missbrauchsgefahr.[239] Im Unterschied zu verkörperten, fassbaren Beweismitteln, lässt sich eine Manipulation elektronischer Beweismittel grundsätzlich nicht unmittelbar erkennen.[240] Möglicherweise wurden die Daten bereits im Vorfeld der Ermittlungsmaßnahmen bearbeitet oder im Rahmen der Ermittlungen durch die Strafverfolgungsbehörden unsachgemäß kopiert und dadurch beweisrechtlich verändert.[241] Verstärkt wird diese Problematik dadurch, dass die beweisrelevanten Daten nicht nur unmittelbar durch den Staat, sondern ebenso durch Privatpersonen erhoben werden können. Gerade im Zusammenspiel mit cloudbasierten Anwendungen sind die entsprechenden Daten auf privaten Servern, etwa bei Amazon, gespeichert. Damit besteht stets das Risiko, dass der private Betreiber auf diese Daten zugreifen kann und diese womöglich verändert.[242] Beweisrechtlich bedeutend sind dabei vor allen Dingen die sog. Metadaten.[243] Hiervon umfasst sind beispielsweise Datum und Uhrzeit der Erstellung eines Dokuments sowie weitere Zusatzinformationen wie Aufnahmeort oder Aufnahmegerät.[244] Solche Metadaten sind jedoch von der Visualisierung eines digitalen Beweismittels nicht umfasst[245] bzw. können durch entsprechende Programme im Vorfeld leicht verändert werden. Darüber hinaus ist zu beachten, dass nicht nur die Metadaten, sondern auch am Computer erstellte Texte, Bilder, Videos oder Tonaufzeichnungen mit zum Teil kostenlosen Programmen auch durch technisch kaum versierte Personen nachträglich verändert werden können.[246] Dieser Unsicherheits-

239 Vgl. BVerfGE 120, 274, 325; *Gercke*, AnwBl 2012, 709, 713.
240 *Sieber*, Verhandlungen des 69. Deutschen Juristentages, C 68.
241 *Sieber/Brodowski* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 19.3, Rn. 164.
242 *Fährmann*, MMR 2020, 228, 230, der darüber hinaus auch kritisch sieht, dass sogar die Bundespolizei, die via Bodycam erhobenen Aufnahmen auf den externen Servern von Amazon speichert, vgl. a.a.O, Fn. 36.
243 Metadaten sind strukturierte Daten, die wiederum Informationen über andere Daten enthalten, vgl. *Grützner/Jakob*, Compliance von A-Z, Metadaten.
244 *Marschall/Herfurth/Winter/Allwin*n, MMR 2017, 152, 153.
245 *Warken*, NZWiSt 2017, 329, 331.
246 *Momsen*, Cybercrime und Cyberinvestigations, 67, 73.

faktor führt dazu, dass sich stets mit der Frage auseinandergesetzt werden muss, woher die vorliegenden Daten stammen, welche Personen Zugriff auf die prozessgegenständlichen Daten hatten, ob sich Veränderungen ausschließen lassen und wer ein Interesse an einer etwaigen Veränderung haben könnte.[247] Um eine vollständige und damit beweisstarke Beweiskette zu erhalten, ist eine möglichst große Nachvollziehbarkeit jedes einzelnen Dechiffrierungsschrittes erforderlich. Problematisch ist dies vor allem bei einer internen Datenverarbeitung durch den Dienstleistungsanbieter, der die Daten sodann in lesbarer Form an die Ermittlungsbehörden übermittelt. Aufgrund dieses internen Vorgangs beim Dienstleister können die Softwareprogramme, mit welchen der Dienstleister die Datenverarbeitung durchführt, daher nicht ohne Verdachtsgrade hinsichtlich einer Manipulation von einem Sachverständigen untersucht werden. In zahlreichen Fällen ist die Richtigkeit der erhaltenen Informationen für die Strafverfolgungsbehörden und auch die Gerichte daher nicht verifizierbar.[248] Obschon der Beweiswert in Folge dieser Punkte vermindert sein kann, ist daraus nicht abzuleiten, dass der Beweiswert elektronischer Daten gegenüber körperlichen Gegenständen oder einer Zeugenaussage stets zurückbleibt. Vielmehr müssen diese Zweifel durch eine sorgfältige Ermittlungsarbeit entkräftet werden, indem im Strafprozess durch die Anklage eine geschlossene Beweismittelkette und -dokumentation vorgelegt wird.[249] Insofern ist darauf hinzuweisen, dass auch körperlichen Beweisgegenständen eine gewisse Unsicherheit anhaftet[250] und auch die Zeugenaussage – wie es bereits die Existenz der §§ 153 ff. StGB verdeutlichen – nicht per se als wahr eingestuft werden darf. Gerichte und Strafverfolgungsbehörden haben darauf zu achten, nicht vorschnell von der Unumstößlichkeit des Wahrheitsgehalts elektronischer Daten ausgehen. Vielmehr und entscheidend ist die freie richterliche Beweiswürdigung hervorzuheben.[251] Es ist und bleibt, gerade auch angesichts einer fortschreitenden Digitalisierung, von der sich auch der Strafprozess nicht befreien kann, ureigenste Aufgabe des Tatrichters, den Wahrheits- und Aussagegehalt eines jeden Beweisstückes, unter Beachtung der Modalitäten des Einzelfalles, zu prüfen und entsprechend zu gewichten. Nicht unerwähnt soll an dieser Stelle bleiben, dass im

247 *Heinson*, IT-Forensik, S. 4.
248 *Warken*, NZWiSt 2017, 329, 330.
249 *Müller*, NZWiSt 2020, 96, 100.
250 *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, 173, 188.
251 Vgl. *Sieber/Brodowski* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 19.3, Rn. 164.

Zusammenspiel mit Sprachassistenten das digitale Beweismittel regelmäßig eine Audioaufzeichnung sein wird. Dies reduziert die Notwendigkeit missbrauchsanfälliger und beweiswertsenkender Transformations- und Bearbeitungsprozesse, da nicht wie beispielweise im Falle der Auswertung von Logfiles oder einer Funkzellenortung der Kerngehalt des Beweismittels erst visualisiert oder wahrnehmbar gemacht werden muss. Gleichwohl darf nicht der Fehler begangen werden, von der scheinbaren Objektivität digitaler Beweismittel auszugehen und die detaillierte Prüfung derselben zu vernachlässigen.[252]

IV) Vor- und Nachteile digitaler Daten als Beweismittel

Ein Vorteil digitaler Beweismittel, der digitalen Daten gemeinhin zukommt, liegt in der unbegrenzten Vervielfältigungsmöglichkeit solcher Dateien. Anders als ein körperliches Beweisstück wie beispielsweise die Tatwaffe, welches als konkreter Gegenstand dem Gericht vorliegt, können elektronische Daten sämtlichen Verfahrensbeteiligten gleichzeitig vorliegen. Dies hat auch zur Konsequenz, dass die Originalaufnahme in der Regel beim Eigentümer verbleiben wird. Es kommt daher nicht zu einem Gewahrsamswechsels hinsichtlich des Beweisstücks. Vielmehr wird eine Datensicherung in Form eines Kopiervorgang auf ein Speichermedium der Behörden durchgeführt.[253] Was für den Betroffenen missliebig, für die Strafverfolgungsbehörden jedoch überaus wertvoll sein kann, ist darüber hinaus der Umstand, dass elektronische Daten durch ein schlichtes Löschen nicht unwiederbringlich beseitigt werden können. Solange die Daten nicht mit neuen Daten überschrieben sind, können entsprechend ausgebildete Beamte diese wiederherstellen und so der Beweisführung zugänglich machen.[254] Mit der Vielfalt elektronischer Daten geht auf der anderen Seite jedoch die Problematik vielfältiger Datenformate einher, die bereits den Bürger im Alltag oftmals vor technische Herausforderungen stellt. Das Konvertieren all dieser Daten in eine für die Verfahrensbeteiligte handhabbare Form bedarf neben der entsprechenden Softwareausstattung vor allen Dingen des notwendigen technischen Knowhows. Diese Komplexität wird durch die beim Bundeskriminalamt und den jeweiligen Landeskriminalämtern eingerichteten Abteilungen zur Aufarbeitung elek-

252 *Momsen*, Cybercrime und Cyberinvestigations, 67, 73.
253 *Warken*, NZWiSt 2017, 289, 294.
254 *Kemper*, ZRP 2007, 105, 108.

tronischer Daten, verdeutlicht.[255] Hinzu kommt, dass das entsprechende Datenmaterial nicht selten eine Größe von mehreren Terabyte aufweist. Dies erfordert zum einen erhebliche technische und vor allen Dingen personelle Ressourcen, um dem im Verfahren geltenden Beschleunigungsgrundsatz hinreichend Rechnung zu tragen.[256] Ebenso kann dies die frühzeitige Selektion der Daten im Sinne einer Reduktion bereits im Ermittlungsverfahren erforderlich machen.[257] Daneben ist zu beachten, dass neben der bereits erwähnten Manipulationsanfälligkeit digitaler Daten die Daten vor einer Sicherung durch die Strafverfolgungsbehörden besonders einfach und schnell verlustig gehen können. Schließlich können elektronische Daten von überall verändert oder gar komplett gelöscht werden. Es ist dabei nicht einmal die physische Anwesenheit am Serverstandort erforderlich, um einen Datensatz zu löschen und damit Spuren zu verwischen.[258] Eine die Strafverfolgungsbehörden vor allem im Rahmen der Beweiserlangung vor größere Schwierigkeiten stellende Herausforderung liegt in der Transnationalität der Speicherorte digitaler Daten. Die Daten werden durch den Nutzer an einen Cloud-Dienstleister übermittelt, der sie auf teilweise weltweit verteilten Servern speichert.[259] Wie bereits einleitend dargestellt, erfolgt auch bei modernen Sprachassistenten die Informationsspeicherung nicht auf dem lokalen Gerät im Eigentum des Betroffenen, sondern auf firmeneigenen Servern. Sofern sich diese Firmen im Ausland befinden, muss, um auf diese Daten zugreifen zu können, nach der aktuellen Gesetzeslage ein internationales Rechtshilfeersuchen eingeleitet werden.[260] Wenngleich solche Nachteile im Vergleich zum „klassischen" körperlichen Beweisgegenstand nicht zu leugnen sind, so kommen die Strafverfolgungsbehörden nicht umher sich diesen Herausforderungen aufgrund der stetig wachsenden Bedeutung und des Umfangs elektronischer Daten – allem voran in Wirtschaftsstrafverfahren – zu stellen.[261]

255 *Warken*, NZWiSt 2017, 329, 331.
256 *Momsen*, Cybercrime und Cyberinvestigations, 67, 75.
257 *Momsen*, Cybercrime und Cyberinvestigations, 67, 75.
258 *Warken*, NZWiSt 2017, 329, 332.
259 *Gercke* in: Gercke/Brunst, Internetstrafrecht, Rn. 40.
260 *Gercke* in: Gercke/Brunst, Internetstrafrecht, Rn. 41; *Brodowski/Freiling*, Cyberkriminalität, S. 173.
261 *Basar/Hiéramente*, NStZ 2018, 681, 681.

§ 4 Zugriffsmöglichkeiten zur Gewinnung elektronischer Daten

In der Strafprozessordnung finden sich eine Vielzahl an heimlichen und offenen Ermittlungsmaßnahmen, die in ihrer Intensität für den Betroffenen ganz unterschiedlich ausgeformt sind. Im Folgenden Kapitel sollen diese Ermächtigungsgrundlagen näher betrachtet werden und sodann unter Beachtung der hierzu ergangenen höchstrichterlichen Rechtsprechung und der sich hierzu in der Literatur entwickelten Strömungen untersucht werden, inwiefern nach aktueller Gesetzeslage auf die durch Sprachassistenten gespeicherten Informationen zugegriffen werden kann.

A. Allgemeines

I) Grundsatz

Das Strafprozessrecht ist zwingend an den verfassungsrechtlich normierten Gesetzesvorbehalt gebunden, da nur dessen Beachtung ein „faires Verfahren" garantieren kann. Es bedarf daher nach der vom BVerfG entwickelten Wesentlichkeitstheorie für jegliche Maßnahmen, die den Betroffenen in seinen verfassungsrechtlich garantierten Rechten zu verletzen drohen, einer gesetzlichen Ermächtigungsgrundlage.[262] Je nach Gewichtung der betroffenen Grundrechte sind an die Erhebung der Daten unterschiedliche Anforderungen zu stellen.[263] Die Bedeutung von Daten und damit auch deren Grundrechtsrelevanz ist ferner abhängig von der Datenart, die terminologisch in TKG und TMG näher beschrieben werden.[264]

262 BVerfG, Beschluss v. 01.03.2000 – 2 BvR 2017/94, Rn. 9.
263 *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 7.
264 *Darby*, Strafverfolgung im Internet, S. 25.

II) Datenarten

Im Zusammenhang mit den bei Telekommunikationsvorgängen relevant werdenden Telekommunikationsdaten wird klassischerweise zwischen Verkehrs-, Bestands- und Inhaltsdaten unterschieden.

1) Bestandsdaten

Gem. § 3 Nr. 3 TGK sind Bestandsdaten die zur Begründung, inhaltlichen Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhobenen Daten, wie den Namen, die Anschrift, die Rufnummer, den Vertragsbeginn oder die Kontodaten. Bestandsdaten geben damit Aufschluss über das Vertragsverhältnis zwischen dem Anbieter der Telekommunikationsdienstleistung und dem Nutzer. Sie sagen noch nichts darüber aus, ob einzelne Leistungen an den Nutzer erbracht wurden. Sie betreffen vielmehr das vertragliche „Grundverhältnis“[265].

2) Verkehrsdaten

Die Verkehrsdaten betreffen die Art des genutzten Kommunikationsdienstes, Anfang Ende und Dauer der Verbindung, das genutzte Datenvolumen, an der Kommunikation beteiligte Personen sowie deren Standorte.[266] Nicht von den Verkehrsdaten erfasst ist der konkrete Inhalt der Kommunikation.[267] In der nahen Vergangenheit sind die Verkehrsdaten im Zuge der Diskussion um die Vorratsdatenspeicherung rechtspolitisch in den Fokus gerückt. Mit den auf diesem Wege erhobenen Daten lassen sich Persönlichkeitsprofile erstellen und das Nutzerverhalten analysieren. Dies soll – so die Befürworter der gesetzlich umstrittenen Regelung[268] – der

265 *Darby*, Strafverfolgung im Internet, S. 25.
266 *Günther* in: MüKo-StPO, G10 § 1, Rn. 22; vgl. im Übrigen die Aufzählung in § 96 TKG.
267 *Günther* in: MüKo-StPO, G10 § 1, Rn. 22.
268 Problematisch ist dabei vor allen Dingen die anlasslose Speicherung der Daten. Vielfach wird bezweifelt, ob die verdachtslose Vorratsspeicherung sämtlicher Verbindungs- und Bewegungsdaten mit den Anforderungen des europäischen Gerichtshofs vereinbar ist. Der Europäische Gerichtshof erklärte 2016 schwedische und britische Gesetze zur verdachtslosen Vorratsdatenspeicherung für

Verhinderung und Aufklärung schwerer Straftaten dienen. Die Erhebung der Verkehrsdaten ist in den §§ 100g StPO, 96 TKG gesetzlich normiert.

3) Inhaltsdaten

Wenngleich sich keine gesetzliche Definition für Inhaltsdaten finden lässt, fällt hierunter jedenfalls der eigentliche Inhalt der ablaufenden Kommunikation.[269] Dabei wird keine Beschränkung auf den klassischen Fall eines Telefongespräches vorgenommen, vielmehr sind auch die konkreten Inhalte einer E-Mail oder eines Messenger-Chats hierunter zu fassen.

4) Zusammenfassung

Anhand dieser Definitionen wird bereits die unterschiedliche Wertigkeit von Daten für die Strafverfolgungsbehörden ersichtlich. Während Bestandsdaten eher von untergeordnetem Interesse sind und zur finalen Aufklärung eines Verbrechens nur selten beitragen können, stellen sich Verkehrs- und vor allem Inhaltsdaten in dieser Hinsicht vielversprechender dar. Gleichwohl sind Bestandsdaten zu Beginn des Ermittlungsverfahren oftmals von Nöten, um erste Anhaltspunkte zur Identifikation einer Person zu erhalten.[270] Während durch die Erhebung von Verkehrsdaten bestimmt werden kann, wo sich eine Person zum Tatzeitpunkt befand, kann nach Erlangen der Inhaltsdaten die komplette Kommunikation zwischen den Betroffenen unter Beachtung der gesetzlichen Grenzen zum Beweis herangezogen werden.

Unter Heranziehung der Verkehrsdaten seines Mobiltelefons verurteilte beispielsweise das LG Hannover einen Angeklagten wegen schwerer

---

nicht mit dem Unionsrecht vereinbar, vgl. EuGH, NJW 2017, 717 ff. Auf nationaler Ebene entschied das Oberverwaltungsgericht Nordrhein-Westfalen, dass das deutsche Gesetz zur Vorratsdatenspeicherung nicht mit Art. 15 Abs. 1 der Datenschutzrichtlinie (2002/58/EG v. 12.07.2002) und damit nicht mit EU-Recht vereinbar sei, vgl. OVG Münster, NVwZ-RR 2018, 43 ff. Die Richter forderten Regelungen, die den betroffenen Personenkreis auf Fälle beschränkten, bei denen ein zumindest mittelbarer Zusammenhang mit der gesetzlich bezweckten Verfolgung und Abwehr schwerer Straftaten bestehe.

269 *Bruns* in: KK-StPO, § 100a StPO, Rn. 15.

270 *Darby*, Strafverfolgung im Internet, S. 25.

Brandstiftung.[271] Dem Angeklagten wurde vorgeworfen, die Wohnung seines Freundes, bei dem er bis zum vorherigen Tag gewohnt hatte, durch Brandlegung zerstört zu haben. Zu seiner Verteidigung führte der Angeklagte aus, dass er den Brand um 19.00 Uhr nicht gelegt haben könne, da er erst die Bahn um 18:55 Uhr ab Hannover zurückgenommen habe und daher um 19:00 Uhr noch gar nicht am Tatort sein konnte. Nach Auswertung der Verkehrsdaten seines Mobiltelefons zeigte sich jedoch, dass der Angeklagte bereits ab 19.00 Uhr mehrfach an einem Funkmast zwischen dem Tatort und dem Bahnhof am Ort des Tatorts eingeloggt war.[272] In einem anderen Fall wurde der Angeklagte wegen Diebstahls und Beihilfe zum Diebstahl verurteilt. Die Überzeugung von der Tatbeteiligung des Angeklagten gewann das urteilende Gericht insbesondere aus den Verbindungsdaten des Mobiltelefons des Angeklagten, die Aufschluss über den jeweiligen Standort des Telefons, Zeitpunkt und Dauer der geführten Telefongespräche und zu den daran beteiligten Anschlüssen gaben.[273] Auf die während eines abgehörten Telefongesprächs gewonnen Inhaltsdaten wurde beispielsweise in einem Fall vor dem LG Stuttgart maßgeblich die Verurteilung wegen unerlaubten Handeltreibens mit Betäubungsmitteln in nicht geringer Menge gestützt.[274] Die Wichtigkeit dieser Daten kann daher aufsteigend von den Bestandsdaten über die Verkehrsdaten hin zu den Inhaltsdaten zusammengefasst werden. Während erstere in der Regel nur zu Beginn des Ermittlungsverfahrens eine Hilfe darstellen, geraten Bestandsdaten und vor allen Dingen Inhaltsdaten im Rahmen der gerichtlichen Beweisführung stärker in den Mittelpunkt. Bei den durch Sprachassistenten gefertigten Audioaufzeichnungen handelt es sich hieran anknüpfend um Inhaltsdaten. Die Aufzeichnungen beinhalten zuvörderst den Inhalt erfolgter Informationsabfragen.

271 LG Hannover, Urteil vom 23.04.2010 – 46 KLs 31/09; die Vorgehensweise zur Beweisgewinnung bestätigend BGHSt 56, 127.
272 BGH, MMR 2011, 412 f.
273 BGHSt 56, 138 (LG Stuttgart, 20.07.2010 – 19 KLs (b) 201 Js 102639/09).
274 BGH, NStZ 2008, 473, 473 (LG Stuttgart).

B. Ermächtigungsgrundlagen

I) § 100a StPO

Der Zugriff auf Telekommunikationsvorgänge erfolgt nach §§ 100a, 100e StPO. Die Normen ermächtigen zu einem Eingriff in das Fernmeldegeheimnis aus Art. 10 GG und das allgemeine Persönlichkeitsrecht, Art 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG.[275] Ob ein Zugriff auch auf die bei der Nutzung eines Smart Speakers ablaufenden Vorgänge möglich ist, richtet sich maßgeblich danach, ob in diesem Vorgang Telekommunikation im Sinne des § 100a StPO gesehen werden kann.

1) Tatbestandsmerkmal der Kommunikation

Eine Legaldefinition der „Telekommunikation" findet sich in der Strafprozessordnung nicht. Gerade in Anbetracht dessen, dass Cloud Computing nicht den Anwendungsfall darstellt, den der Gesetzgeber bei Schaffung des § 100a StPO vor Augen hatte, ist auch bis heute nicht hinreichend geklärt, inwiefern bei einer Verbindung des Nutzers mit dem Cloud-Dienst von Telekommunikation gesprochen werden kann. Entscheidend ist insofern auch, wie der Telekommunikationsbegriff aus § 100a StPO zu verstehen ist.

a) Weiter technischer Telekommunikationsbegriff

Allem voran in der Rechtsprechung entwickelte sich ab Mitte der 90er Jahre ein technisch geprägter Telekommunikationsbegriff.[276] Einfach gesetzlich wird dabei an § 3 Nr. 22 TKG angeknüpft, nach dessen Legaldefinition unter Kommunikation „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen" zu verstehen ist. Argumente für diese Sichtweise werden vor allem mit Blick auf den gesetzgeberischen Willen vorgebracht. So soll im Zuge der Änderung des Wortlauts des § 100a StPO von „Fernmeldeverkehr" zu „Telekommunikation" zum Ausdruck gebracht worden sein, dass mit dieser Angleichung an die Terminologie des TKG die Begriffe auch inhaltlich

275 *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 24.
276 BGH, NJW 2003, 2034 f.; BGH, NJW 2007, 930, 931 f.

gleich auszulegen seien.[277] Wenngleich in diesem Lager Einigkeit herrscht, den Kommunikationsbegriff im Einklang mit dem TKG zu bestimmen, so können dennoch unterschiedliche Ausprägungen dieser weiten Sichtweise erkannt werden.[278]

aa) Technische Auslegung

Anhänger der rein technischen Auffassung greifen zur Bestimmung der Kommunikation ausschließlich und ohne etwaige Einschränkungen auf § 3 Nr. 22 TKG zurück. Ausweislich der hierfür einschlägigen Definition kann Telekommunikation auch zwischen bloßen Maschinen stattfinden; eine menschliche Teilhabe ist an dem Kommunikationsprozess überhaupt nicht erforderlich. Dies wird damit begründet, dass letztlich selbst die Kommunikation zwischen zwei Maschinen auf einen menschlichen Ursprung zurückgehe. Durch einen Befehl zur Ausführung oder das anfängliche Programmieren der Maschinen beruhe auch die durch Maschinen ablaufende Kommunikation mittelbar auf menschlichem Handeln.[279]

bb) Technikorientierte Auslegung

In die gleiche Richtung gehen die Rechtsprechung des Bundesgerichtshofs und große Teile der Literatur, die sich ebenfalls an der Legaldefinition des TKG orientieren.[280] Fortlaufend wird dabei betont, dass die Begriffe Telekommunikation in § 100a StPO und § 3 Nr. 22 TKG inhaltsgleich zu verstehen sein sollen.[281] Gleichwohl soll nicht jeder technische Vorgang des Aussendens, Übermittelns oder Empfanges von § 100a StPO erfasst sein. Dies solle nur für solche Vorgänge gelten, die mit der Nachrichtenübermittlung mittels Telekommunikationsanlagen im Zusammenhang

277 *Meininghaus*, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, S. 79.
278 Ähnlich bereits *Grözinger*, Die Überwachung von Cloud-Storage, S. 182.
279 *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 266; *Meininghaus*, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, S. 79.
280 *Klesczewski*, ZStW 2011, 737, 741; *Schmitt* in: Meyer-Goßner/Schmitt, § 100a StPO, Rn. 6.
281 BGH, StV 2003, 370, 371; *Hauck* in: LR-StPO, § 100a StPO, Rn. 29; *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 3; *Eschelbach* in: SSW-StPO, § 100a StPO, Rn. 2; *Schmitt* in: Meyer-Goßner/Schmitt, § 100a StPO, Rn. 6.

stehen.[282] Dabei wird auch der Begriff der Telekommunikationsanlage anhand der Legaldefinition aus § 3 Nr. 23 TKG abgeleitet. „Telekommunikationsanlagen" sind technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Damit ein Vorgang daher unter § 100a StPO fallen könne, ist Voraussetzung, dass wenigstens eine Person mittels einer solchen Telekommunikationsanlage kommuniziere. Bei dieser Person soll jedoch wiederum nicht von Relevanz sein, ob sich der aktuelle Kommunikationsvorgang mit Wissen und Willen des Betroffen vollzieht.[283]

b) Grundrechtsanaloger Telekommunikationsbegriff

Eine andere Strömung will den Telekommunikationsbegriff analog zu Art. 10 Abs. 1 Var. 3 GG verstanden wissen.[284] Durch diese Auslegung der Ermächtigungsgrundlage soll ein möglichst umfassender Schutz des Fernmeldegeheimnisses aus Art. 10 GG gewährleistet werden.[285] Ihre Berechtigung soll diese Sichtweise darin finden, dass § 100a StPO in seiner ursprünglichen Fassung von der Überwachung des „Telekommunikationsverkehrs" ausgegangen ist, nun aber die gleiche Terminologie wie Art. 10 Abs. 1 Var. 3 GG, der vom „Telekommunikationsgeheimnis" spricht, nutzt.[286] Dadurch komme zum Vorschein, dass der Gesetzgeber eine Ermächtigung für die Überwachung sämtlicher von Art. 10 Abs. 1 Var. 3 GG geschützter Verhaltensweisen schaffen wollte.[287] Zudem sei zu beachten, dass auch bei einer solchen extensiven Auslegung der Ermächtigungsgrundlage der Schutz vor staatlichen Eingriffen nicht leelaufen würde. Denn gem. § 100a Abs. 1 StPO darf eine Überwachung und Aufzeichnung der Kommunikation nur dann erfolgen, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen hat. Ein notwendiges Anordnungserfordernis ist demnach der Verdacht, dass eine der hier abschlie-

282 BGH, StV 2003, 370, 371.
283 BGH, StV 2003, 370, 372.
284 *Wölm*, Schutz der Internetkommunikation und heimliche Internetaufklärung, S. 243; *Bruns* in: KK-StPO, § 100a StPO, Rn. 4; *Dalby*, Strafverfolgung im Internet, S. 93; Gaede, StV 2009, 96, 100.
285 LG Aachen, StV 1999, 590.
286 *Grözinger*, Die Überwachung von Cloud-Storage, S. 211.
287 *Grözinger*, Die Überwachung von Cloud-Storage, S. 211.

ßend aufgeführten Straftaten vorliegen könnte. Dabei ist es ausreichend, dass es nach kriminalistischer Erfahrung möglich erscheint, dass eine verfolgbare Straftat vorliegt (Anfangsverdacht)[288]. Es bedarf weder eines hinreichenden Tatverdachts[289], daher der einfachen Wahrscheinlichkeit einer Verurteilung,[290] noch eines dringenden Tatverdachts,[291] in Form einer hohen Wahrscheinlichkeit, dass der Beschuldigte als Täter oder Teilnehmer rechtswidrig und schuldhaft eine Straftat begangen hat[292]. Als weitere Einschränkung muss die Tat gem. § 100a Abs. 1 Nr. 2 StPO auch im Einzelfall schwer wiegen und die Erforschung des Sachverhalts muss auf andere Weise wesentlich erschwert oder aussichtslos wäre (sog. Subsidiaritätsklausel).

c) Enger strafverfahrensrechtlicher Telekommunikationsbegriff

Zuletzt wird für ein Lossagen von Einflüssen aus dem Grundgesetz oder dem TKG plädiert und eine eigenständige strafprozessuale Auslegung des Telekommunikationsbegriffes favorisiert.[293] Erstmalig aufgekommen ist die Frage nach einem genuin zu bestimmenden Telekommunikationsbegriff im Anschluss an den Beschluss eines BGH-Ermittlungsrichters betreffend den staatlichen Zugriff auf die in einer Mailbox gespeicherten Computerdaten.[294] In dem Beschluss vom 31.07.1995 erlaubte der zuständige Ermittlungsrichter über § 100a StPO den Zugriff auf die Mailbox des Betroffenen, ohne nähere Ausführungen zu der Frage, inwiefern bei den auf der Mailbox gespeicherten Daten noch von Fernmeldeverkehr i.S.d. § 100a a.F. StPO gesprochen werden kann.[295] Dadurch kam die Befürchtung auf, dass in der Entscheidung von der Eröffnung des grundrechtlichen Schutzbereich auf das Vorliegen einer tatbestandlichen Voraussetzung des Gesetzesvorbehalts geschlossen wurde.[296] Die sich sodann entwickelnde Strö-

288 *Beulke/Swoboda*, Strafprozessrecht, Rn. 172.
289 Vgl. §§ 170 Abs. 1, 203 StPO.
290 *Schmitt* in: Meyer-Goßner/Schmitt, § 203 StPO, Rn. 2.
291 Vgl. §§ 111a Abs. 1, 112 StPO.
292 *Roxin/Schünemann*, Strafverfahrensrecht, § 30, Rn. 5.
293 *Gercke* in: HK-StPO, § 100a StPO, Rn. 10; *ders.*, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, S. 98 f.; *Hiéramente,* HRRS 2016, 448, 450; *Demko*, NStZ 2004, 57, 61; *Roggan*, NJW 2015, 1995, 1996; *Bernsmann/Jansen*, StV 1999, 591; *Eschelbach* in: SSW-StPO, § 100a StPO, Rn. 5.
294 *Kudlich*, JuS 1998, 209, 213 f.
295 BGH (Beschluss des Ermittlungsrichter), NJW 1997, 1934.
296 *Kudlich*, JuS 1998, 209, 213 f.

mung war sich insofern einig, den Telekommunikationsbegriff anhand der gängigen Auslegungsmethoden unter Berücksichtigung der strafprozessualen Besonderheiten zu bestimmen.[297] Eine genauere Darstellung wie ein solcher Telekommunikationsbegriff sodann auszuformulieren wäre, findet sich jedoch nur selten. *Hiéramente* stellt im Zuge dieser Definitionsentwicklung das Erfordernis einer sozialen Interaktion in den Mittelpunkt.[298] Nur so könne dem Umstand Rechnung getragen werden, dass der Betroffene auch unter den Schutz des Art. 10 GG fallende Tätigkeiten verüben könne, ohne dabei freiwillig auf seine Privatsphäre zu verzichten. Beispielhaft dafür sei die gerade nicht öffentlich ablaufende Nutzung des Internets zur Informationsgewinnung, bei welcher – im Unterschied zur klassischen Telekommunikation im Rahmen eines Telefongesprächs – keine soziale Interaktion stattfinde. Bei der klassischen Telekommunikation offenbare der Betroffene im Rahmen eines Telefongesprächs, einer E-Mail oder im Chat bewusst und freiwillig Wissen gegenüber einem Dritten.[299] Die Nutzung des Internets zum Zwecke der reinen Informationsgewinnung erfordert hingegen keine Interaktion mit Dritten und ist, jedenfalls solange die Informationen nicht in öffentlichen frei zugänglichen Foren oder Chats geteilt werden, seiner Natur nach ein privater Vorgang. Andere wiederum stellen entscheidend darauf ab, dass die Kommunikation mit einem Mitteilungswillen erfolgen müsse.[300]

2) Nutzung eines Smart Speakers als Kommunikation i.S.d. § 100a Abs. 1 S. 1 StPO

Zur Beantwortung der Frage, ob die Nutzung eines Smart Speakers Telekommunikation i.S.d. § 100a StPO darstellt, ist entscheidend zu welchem Zeitpunkt die Nutzung des Sprachassistenten überwacht wird.[301] Dabei kann in das Stadium vor der Datenübertragung, während der Übertragung und nach der Übertragung der Daten unterschieden werden. Eine ähnliche Unterscheidung wurde grundlegend bereits zur Bestimmung der

297 *Gercke* in: HK-StPO, § 100a StPO, Rn. 10; *Fezer*, NstZ 2003, 625, 627.
298 *Hiéramente,* StraFo 2013, 96, 99.
299 *Hiéramente,* HRRS 2016, 448, 451.
300 *Wicker*, Cloud Computing und staatlicher Strafanspruch, S. 380.
301 Diese zutreffende Differenzierung bzgl. der Nutzung von Cloud-Speichern wie Dropbox, iCloud oder Google Drive bereits bei *Grözinger*, Die Überwachung von Cloud-Storage, S. 188 ff.

Ermächtigungsgrundlage hinsichtlich des Zugriffs auf den E-Mail-Verkehr herangezogen.[302]

a) Vor der Übertragung

Vor der Übertragung der aufgezeichneten Sprachnachricht scheidet ein Zugriff auf das Endgerät des Nutzers nach § 100a StPO sowohl nach der rein technischen als auch nach der technikorientierten Auffassung aus. Dem Aussenden, Übermitteln und Empfangen wie es in § 3 Nr. 22 TKG heißt, ist ein dynamischer Übermittlungsvorgang immanent. An einem solchen fehlt es, wenn sich die Audioaufzeichnungen bildlich gesprochenen noch nicht auf dem Weg zum Server des Sprachassistenten befinden, sodass keine Telekommunikation i.S.d. § 22 Nr. 3 TKG vorliegt. Auch ist zu diesem Zeitpunkt der Schutzbereich des Art. 10 GG noch nicht eröffnet. Die Daten befinden sich noch auf dem Gerät des Nutzers und damit noch in dessen Herrschaftssphäre. Vor Beginn des Übertragungsvorgangs ist vielmehr der Schutzbereich des Art. 2 Abs. 1 GG i.V.m. Art. 1 GG betroffen.[303] Zu einer Übertragung aufgrund oder infolge derer einfacher auf die Daten zugegriffen werden könnte, kam es zu diesem frühen Zeitpunkt noch nicht. Insofern ist Art. 10 GG, dem nur die Vertraulichkeit des zur Nachrichtenübermittlung eingesetzten Übertragungsmediums unterfällt[304], in diesem Stadium noch nicht einschlägig. Auch im Sinne eines strafprozessualen Telekommunikationsbegriffes liegt zu diesem Zeitpunkt noch keine Telekommunikation vor. Als Mindestanforderung verlangt auch dieser einen dynamischen Übermittlungsvorgang.

b) Während des Übertragungsweges

Deutlich interessanter erscheint aus dem Blickwinkel des § 100a StPO der zeitliche Teil der Übermittlung der Audioaufzeichnungen zum Server, bevor dort mittels Algorithmen die Spracheingaben in – für den Sprachassistenten – verwertbare Daten umgewandelt werden.

---

302 Vgl. bzgl. der aufgestellten Phasen *Schlegel*, HRRS 2007, 44, 47; *Beulke/Swoboda*, Strafprozessrecht, Rn. 392; *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 55; *Klesczewski*, ZStW 2011, 737, 744 ff.; *Zimmermann*, JA 2014, 321 f.

303 BT-Drs. 18/12785, S. 49.

304 BVerfG, NJW 2002, 3619, 3621.

aa) Rein technische Auslegung

Im Lichte eines rein technischen Verständnisses des Telekommunikationsbegriffes wäre die Nutzung eines Sprachassistenten als Kommunikation i.S.d. § 100a StPO aufzufassen, sofern diese unter § 3 Nr. 22 TKG subsumierbar ist. Das Aussenden, Übermitteln und Empfangen beziehen sich auf jegliche Signale. Auf den Inhalt oder den Zweck der Signale kommt es nicht an. Entscheidend ist damit ausschließlich, ob eine technische Übertragungsleistung vorliegt, was unabhängig vom Übertragungsdienst und dem Inhalt der Übertragung zu beurteilen ist.[305] Den Signalen muss lediglich ein beliebiger Informationsgehalt zukommen, die sie als Nachricht identifizierbar machen und als solche Daten transportieren.[306] Der Übertragungsvorgang müsste wie sich aus § 3 Nr. 22 TKG ergibt mittels einer Telekommunikationsanlage i.S.d. § 3 Nr. 23 TKG erfolgen.

Das Endgerät eines Sprachassistenten zeichnet das gesprochene Wort auf, sodass dieses als gespeicherte Audiodatei via Internet an das Rechenzentrum bzw. die Cloud des Anbieters übermittelt werden kann. In dieser Übermittlung ist zweifelsohne eine Übertragungsleistung zu sehen, weshalb die transportierten Audioaufzeichnungen als Kommunikation i.S.d. §§ 22, 23 TKG einzuordnen sind, sofern auf den Datenstrom zwischen dem Nutzer des Sprachassistenten und dem verarbeitenden Server zugegriffen wird.

bb) Technikorientierter Telekommunikationsbegriff

Unabhängig davon, dass während des Übertragungsweges bei der Nutzung eines Sprachassistenten von Kommunikation i.S.d. §§ 22, 23 TKG gesprochen werden kann, müsste im Sinne der technikorientierten Auffassung der Betroffene einschränkend gerade mittels einer Telekommunikationsanlage kommunizieren wollen. Es ist daher zu klären, ob der Nutzer eines Sprachassistenten mittels diesem kommunizieren will oder durch die Aktivierung des Sprachassistenten lediglich eine Datenübermittlung von technischem Gerät zu technischem Gerät stattfindet. Zur Beantwortung dieser Frage eignet sich ein Blick auf einem ähnlich gelagerten Fall und die hierzu ergangene Rechtsprechung. Die bei der Nutzung eines Sprachassistenten ablaufende „Kommunikation im weitesten Sinne“ ist in

305 *Fetzer* in: Arndt/Fetzer/Scherer/Graulich-TKG, § 3, Rn. 100.
306 *Lünenberger/Stamm* in: Scheurle/Mayen-TKG, § 3, Rn. 61.

der Regel darauf gerichtet eine Antwort auf eine dem Sprachassistenten gestellte Frage zu erhalten. Der gleiche Ablauf findet sich in der Sache beim Surfen im Internet und der Nutzung einer Suchmaschine zur Informationsbeschaffung. Nach Ansicht des LG Ellwangen, stellt auch die Nutzung des Internets durch Abruf von Web-Seiten im World Wide Web mittels eines Web-Browsers eine Internetkommunikation und damit eine Telekommunikation im Sinne strafprozessualer Vorschriften dar.[307] Die Vertreter dieser Sichtweise argumentieren, dass es beim Abruf von Informationen im Internet im Rahmen des Googelns gerade nicht lediglich zu einem bloßen technischen Austausch von Datenpaketen zwischen informationstechnischen Systemen komme, sondern es sich bei den gewonnen Daten um bewusst von Personen zu Kommunikationszwecken eingegebene und abgerufene Informationen handle.[308] In der Eingabe von Suchbegriffen in einer Internetsuchmaschine wie Google könne daher Telekommunikation im Sinne des § 100a StPO liegen. Überträgt man diese Rechtsprechung auf den hiesigen Fall so müsste auch die Nutzung eines Sprachassistenten als Kommunikation i.S.d. § 100a StPO anzusehen sein.[309]

cc) Grundrechtsanaloger Telekommunikationsbegriff

Um aus Sicht eines grundrechtsanalogen Telekommunikationsbegriffes zu bestimmen, ob während des Übermittlungsvorgangs Telekommunikation vorliegt, ist bereits an dieser Stelle näher auf den sachlichen Schutzbereich des Art. 10 GG einzugehen und sodann zu fragen, ob die Nutzung eines Sprachassistenten während des Übermittlungsvorganges hierunter fällt.

(1) Grundsätzliches

In der Sache schützt Art. 10 Abs. 1 Var. 3 GG die unkörperliche Übermittlung von Informationen an individualisierte Empfänger mit Hilfe des Telekommunikationsverkehrs.[310] Der Schutzzweck des Art. 10 GG liegt

307 LG Ellwangen, Beschl. v. 28.05.2013, Az.: 1 Qs 130/12.
308 *Bär*, ZD 2017, 132, 137.
309 Im Ergebnis *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 99; offenlassend, ob dabei Telekommunikation vorliegt BT-Drs. 19/11478, S. 3.
310 BVerfGE 115, 166, 182; *Hermes* in: Dreier-GG, Art. 10 GG, Rn. 37; *Schoch*, JURA 2011, 194, 197.

darin begründet, dass bei einer Kommunikation über eine räumliche Distanz die Gesprächspartner – im Gegenteil zu einem Gespräch unter Anwesenden – nicht die Möglichkeit haben, den äußeren Rahmen der Kommunikation alleine zu bestimmen und über die Privatheit und die Gesprächsbeteiligten selbst zu wachen.[311] Vielmehr ist aufgrund der räumlichen Distanz ein technischer Übermittlungsvorgang erforderlich, auf den der zu schützende Bürger keinen Einfluss hat. Der dabei bestehenden Gefahr, dass sich Dritte aufgrund technischer Möglichkeiten, Zugang zu den Inhalten und Übermittlungsdaten der Kommunikation verschaffen, soll so entgegengewirkt werden.[312] Als Abwehrrecht schützt Art. 10 GG vor einer staatlichen Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation und so vor Gefahren für die Vertraulichkeit von Mitteilungen, die aus dem Übermittlungsvorgang einschließlich der Einschaltung fremder Übermittler entstehen.[313] Dabei kommt es weder auf die konkrete Übermittlungsart (Kabel, Funk, analoge oder digitale Vermittlung) noch die gewählte Ausdrucksform (Sprache, Bilder, Töne oder sonstige Daten) an.[314] Zu Recht wurde bezüglich des Schutzbereichs aus Art. 10 GG höchstrichterlich festgestellt, dass der Schutzbereich zum Schutz der Bürgerinnen und Bürger gegenüber neuen technischen Entwicklungen offen ist. Der sachliche Schutzbereich findet seine Grenze also nicht in den zu einem bestimmten Zeitpunkt bekannten und sich im Einsatz befindlichen Arten elektronischer Informationsvermittlung. Insofern wird von einer dynamischen und entwicklungsoffenen Grundrechtsgewährleistung gesprochen.[315] Beispielsweise werden E-Mails, SMS, Messenger-Dienste und Chats dem Fernmeldegeheimnis und nicht dem Briefgeheimnis zugeordnet.[316]

311 BverfGE 106, 28, 36.
312 BverfGE 106, 28, 36.
313 BverfGE 106, 28, 36 f.
314 BverfGE 115, 166, 182 f.; *Sodan* in: Sodan-GG, Art. 10 GG, Rn. 5; *Hermes* in: Dreier-GG, Art. 10 GG, Rn. 36; *Guckelberger* in: SHH, Art. 10 GG, Rn. 22.
315 BverfGE 115, 166, 182; *Durner* in: Maunz/Dürig-GG, Art. 10 GG, Rn. 64; *Pagenkopf* in: Sachs-GG, Art. 10 GG, Rn. 14b; *Sodan* in: Sodan-GG, Art. 10 GG, Rn. 5; *Guckelberger* in: SHH, Art. 10 GG, Rn. 21 f.; *Martini* in: v. Münch/Kunig, Art. 10 GG, Rn. 63.
316 *Morlok*, Grundrechte, Rn. 324.

(2) Sinn und Zweck der Grundrechte

Für die stets wiederkehrende Frage, inwiefern ein bestimmtes Verhalten unter den Schutz eines Grundrechts fällt, wird im Folgenden Sinn und Zweck der Grundrechte bemüht. Daher ist fraglich, was eigentlich Sinn und Zweck der Grundrechte darstellt. Eine richtungsweisende Antwort auf diese Frage findet sich bereits in der Lüth-Entscheidung aus dem Jahre 1958. Dort heißt es *„ohne Zweifel sind die Grundrechte in erster Linie dazu bestimmt, die Freiheitssphäre des einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern*“[317]. In der Folge entwickelte sich eine Differenzierung in Freiheitsgrundrechte bzw. Abwehrgrundrechte, zur Abwehr eines staatlichen Handelns und Leistungsgrundrechte mit deren Hilfe ein staatliches Handeln erzwingbar werden sollte. Bei dem hier in Rede stehenden Art. 10 GG handelt es sich um ein sog. Freiheitsgrundrecht, mit der Zielsetzung, dass der Staat es unterlässt, auf den Fernmeldeverkehr bzw. die Telekommunikation zuzugreifen. Ein solches Abwehrgrundrecht hat das Ziel, die Freiheit vor staatlichen Zugriffen zu gewährleisten, stellt also den sog. status negativus dar.[318] Sofern es bereits zu einem staatlichen Eingriff gekommen ist wird der abwehrende Charakter der Freiheitsgrundrechte dadurch deutlich, dass sich aus dem Grundrecht ein Beseitigungsanspruch ergibt.[319] Hinsichtlich Art. 10 GG hat das BVerfG mehrfach betont, dass das Grundrecht zur Bestimmung seines Schutzgehalts an den Grundrechtsträger und dessen Schutzbedürftigkeit anknüpfen muss.[320] Daher ist für die Bestimmung der Reichweite von Art. 10 GG stets zu fragen, wovor der Grundrechtsträger geschützt werden soll und ob dieser in einer konkreten Situation aufgrund seiner Machtlosigkeit gegenüber dem Staat verfassungsrechtlich garantierten Schutz bedarf.

(3) Massen- oder Individualkommunikation

Eine grobe Unterteilung, ob ein Verhalten unter den Schutz des Art. 10 GG fällt, kann durch eine Unterscheidung zwischen Massen- und Individualkommunikation vorgenommen werden. Nur im Falle von Indi-

317 BverfGE 7, 198, 204.
318 *Hufen*, Grundrechte, § 5, Rn. 1.
319 *Jarass* in: Handbuch der Grundrechte, § 38, Rn. 16.
320 BverfGE 124, 43, 56; BVerfG, NJW 2007, 351, 354; *Hartmann* in: HK-GS, § 100a StPO, Rn. 2.

vidualkommunikation soll der Schutzbereich eröffnet sein. Hinsichtlich der Massenkommunikation, die an einen unbestimmten Rezipientenkreis gerichtet ist, wird angenommen, dass solche öffentliche Kommunikationsvorgänge nicht als vertraulich eingestuft werden können und damit nicht dem Schutz des Fernmeldegeheimnisses unterfallen.[321] Ursprünglich sollte diese Abgrenzung vor allem den Unterschied zwischen Rundfunk- und Telekommunikationsfreiheit verdeutlichen.[322] Gleichfalls wird sie aber auch zur Differenzierung innerhalb einer möglichen Betroffenheit des Art. 10 GG genutzt. Vor allen Dingen in der neueren Literatur wird zur Abgrenzung zwischen Individual- und Massenkommunikation auf die Art der Anwendung[323] oder auf das Vorhandensein etwaiger Zugangshindernisse abgestellt[324]. Während die Nutzung des World Wide Web aufgrund des ungehinderten Zugangs eher der Massenkommunikation zuzuordnen wäre, würde es sich bei der Versendung einer E-Mail vielfach um Individualkommunikation handeln. Eine solche Abgrenzung ist angesichts der technischen Gegebenheiten der über das Internet ablaufenden Telekommunikation jedoch ohnehin nicht zielführend, da ihr handfeste Abgrenzungskriterien fehlen.[325] So kann die E-Mail tatsächlich als Äquivalent postalischer Fernkommunikation und damit als Individualkommunikation angesehen werden, gleichzeitig bei Verwendung zur Versendung eines Newsletters aber auch der Massenkommunikation zuzuordnen sein.[326] Es würde sich unmittelbar die Frage anschließen, ab welcher Personenanzahl von einem unbestimmten Rezipientenkreis auszugehen wäre. Letztlich findet sich selbst im Falle der Versendung eines Newsletters mittels einer E-Mail ein in sich abgeschlossener Personenkreis als Empfänger der Nachricht wieder. Klarer wird diese Abgrenzung auch nicht durch Heranziehung des Kriteriums eines „Zugangshindernisses". Es bleibt unklar, wie ein solches Zugangshindernis praktisch ausgestaltet sein muss. Ist es lediglich die Eintragung in eine Maillingsliste zum Erhalt eines Newsletters, die aus der Massen- eine Individualkommunikation macht? Muss es sich bei offen einsehbaren Kommentierungen in sozialen Netzwerken, die ersichtlich mit Verzicht auf Vertraulichkeit getätigt wurden, dennoch um Individualkommunikation handeln, da schließlich für diese Netzwerke eine

321 *Gusy* in: v. Mangoldt/Klein/Stark, Art. 10 GG, Rn. 62; *Sankol*, MMR 2006, 361, 364.
322 *Gusy* in: v. Mangoldt/Klein/Stark, Art. 10 GG, Rn. 62.
323 *Sievers*, Der Schutz der Kommunikation im Internet, S. 129, m.w.N.
324 *Hermes* in: Dreier-GG, Art. 10 GG, Rn. 39.
325 *Guckelberger* in: SHH, Art. 10 GG, Rn. 23.
326 *Greve*, Acces-Blocking, S. 293.

Registrierung erforderlich ist und mithin ein Zugangshindernis besteht? Aus praktischen Gesichtspunkten schon gar nicht durchsetzbar ist diese Abgrenzung nicht zuletzt deswegen, da die zur Abgrenzung benötigten Informationen gewonnen werden müssten, ohne den Inhalt der übermittelten Nachricht einzusehen.[327] Hinzu kommt, dass selbst der Abruf frei zugänglicher Internetseiten die Herstellung einer individuellen Verbindung verursacht.[328]

In die gleiche Kerbe schlägt das BVerfG, wenn es auf diese Differenzierung verzichtet und vielmehr eine den konkreten Einzelfall betrachtende Sichtweise anlegt, die für entscheidend hält, ob die Kommunizierenden die ablaufende Kommunikation vertraulich wissen wollten.[329] Es ist festzuhalten, dass wenngleich es sich bei der Nutzung eines Sprachassistenten keineswegs um Massenkommunikation handelt, die dessen Nutzung aus dem Schutzbereich des Art. 10 GG herausnehmen würde, diese Abgrenzung bei den vielfältigen Kommunikationsmöglichkeiten über das Internet nur schwerlich anzuwenden ist.

(4) Teilnehmer an einem Kommunikationsvorgang

Fraglich ist, ob für einen Telekommunikationsvorgang im Sinne des Art. 10 GG hieran mindestens zwei Personen beteiligt sein müssen.

(4.1) Entwicklung der Rechtsprechung

Zwar hat sich das BVerfG in seiner Rechtsprechung zu Art. 10 GG noch nicht ausdrücklich hinsichtlich der Frage, ob es für die Schutzbereichseröffnung mindestens zweier Personen bedarf, geäußert. Aus diversen Entscheidungen, die im Nachfolgenden genauer betrachtet werden sollen, lassen sich jedoch Anknüpfungspunkte und Tendenzen erkennen.

327 *Sievers*, Der Schutz der Kommunikation im Internet, S. 130.
328 *Sievers*, Der Schutz der Kommunikation im Internet, S. 130.
329 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 37 = teilweise in NJW 2016, 3508 ff.

(4.1.1) Auslesen eines Endgerätespeichers

In einer Entscheidung, das Auslesen einer SIM-Karte betreffend, hat das BVerfG entschieden, dass auch die auf einer SIM-Karte des eigenen Handys gespeicherten Informationen dem Schutzbereich des Art. 10 GG zuzuordnen sind.[330] Einleitend betonte das Bundesverfassungsgericht, dass das Grundrecht aus Art. 10 GG neuen technischen Entwicklungen gegenüber offen sei und sich auf sämtliche Übermittlungen beziehe, die unter Zuhilfenahme der verfügbaren Telekommunikationstechniken vonstattengehen.[331] Gleichwohl finden sich in der Entscheidung Passagen, die auf die Beteiligung zweier miteinander Kommunizierender Personen schließen lassen: "[…] *wenn diese wegen der räumlichen Distanz zwischen den Beteiligten* […]"[332] oder „*die Kommunizierenden müssen sich auf die technischen Besonderheiten eines Kommunikationsmediums einlassen und sich dem eingeschalteten Kommunikationsmittler anvertrauen* […]"[333]. Neben dem Erfordernis eines Kommunikationsmittlers scheint das Bundesverfassungsgericht daher auch die Notwendigkeit von „Beteiligten" bzw. „Kommunizierenden" für eine Schutzbereichseröffnung für erforderlich zu halten. Relativiert wird die vermeintliche Betonung der personalen Komponente jedoch durch die Formulierung, dass der Schutz durch Art. 10 GG gerade einen Ausgleich für die technikbedingt notwendigerweise in Kauf genommene Einbuße an Privatheit schaffe, um den Gefahren zu begegnen, die sich gerade aus dem technischen Übermittlungsvorgang ergeben.[334] Darüber hinaus knüpfe das Fernmeldegeheimnis an das verwendete Kommunikationsmedium an.[335] Daraus könnte zu schließen sein, dass es der Intention des Bundesverfassungsgerichts entspricht, unabhängig von der Anzahl der konkret am Telekommunikationsvorgang beteiligten Personen, die Gefahr abzuwenden, die sich speziell aufgrund der Einschaltung eines Nachrichtenmittlers ergibt.[336]

330 BverfGE 115, 166.
331 BverfGE 115, 166, 182 f.
332 BverfGE 115, 166, 182.
333 BverfGE 115, 166, 184.
334 BverfGE 115, 166, 184; BVerfG, NJW 2007, 351, 353.
335 BverfGE 100, 313, 363; BverfGE 115, 166, 184.
336 *Kleih*, Die strafprozessuale Überwachung der Telekommunikation, S. 113.

(4.1.2) IMSI-Catcher Beschluss

In der genannten Entscheidung befasste sich das Bundesverfassungsgericht mit der Frage, ob die durch einen IMSI-Catcher erlangten Daten dem Schutzbereich des Art. 10 GG unterfallen. In technischer Hinsicht ist es allen Mobiltelefonen immanent, dass sich diese, sofern sie sich im empfangsbereiten Zustand befinden, in kurzen Abständen immer wieder in die für sie zuständige Basisstation des Mobilfunknetzwerkes einwählen. Diesen Umstand können sich gem. § 100i StPO die Strafverfolgungsbehörden durch den Einsatz eines IMSI-Catchers zu Nutze machen. Durch dessen Einsatz wird ein solches Mobilfunknetzwerk simuliert, in welches sich alle Mobiltelefone in einem gewissen Umkreis aufgrund des von dem Netzwerk ausgehenden Signals einwählen.[337] Indem nun sämtliche eingeschalteten Mobiletelefone ihre Daten an dieses simulierte Netzwerk senden, kann die auf der SIM-Karte gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle näher bestimmt werden.[338] Die Beschwerdeführer brachten dabei vor, dass das Telekommunikationsgeheimnis nicht nur den Inhalt einer Kommunikation, sondern darüber hinaus auch alle weiteren Umstände, wie Gerätenummer oder Standortdaten, die mit einer solchen Kommunikation in Zusammenhang stünden, schütze.[339] Dieser Sichtweise ist das BVerfG entgegengetreten. Art. 10 GG schütze gerade die individuelle Kommunikation zwischen den Beteiligten in den Fällen, in denen aufgrund der räumlichen Distanz eine Übermittlung durch Dritte erforderlich ist.[340] Beim Einsatz eines IMSI-Catchers fehle es jedoch an diesen Voraussetzungen, da in dieser Situation ausschließlich technische Geräte miteinander kommunizieren. Es fehle folglich an einem menschlich veranlassten Kommunikationsvorgang.[341] Der Umstand, dass Mobiltelefone Daten aussenden, die sich die Strafverfolgungsbehörden im vorliegenden Fall zu Nutze machten, erfolgte unabhängig von einem konkreten Kom-

337 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 13 f. = teilweise in NJW 2007, 351 ff.
338 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 14 = teilweise in NJW 2007, 351 ff.
339 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 23 = teilweise in NJW 2007, 351 ff.
340 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 51 = teilweise in NJW 2007, 351 ff.
341 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 57 = teilweise in NJW 2007, 351 ff.

munikationsvorgang. Da erst die tatsächliche Nutzung eines Mobiltelefons zum Informationsaustausch die übertragenen Daten als Kommunikationsinhalt qualifiziere, hat das BVerfG entschieden, dass der reine technische Datenaustausch zwischen Mobilfunkendgeräten nicht dem Schutzbereich des Art. 10 GG unterfallen.[342]

Vergleicht man diese Fallgestaltung mit der Nutzung eines Smart Speakers, ist zu erkennen, dass durch die Übermittlung, der durch das Gerät vor Ort aufgenommenen Audiodatei an den Sprachassistenten letztlich auch ein bloßer Austausch von Datenpaketen stattfindet. Jedoch ist für die Eröffnung des Schutzbereiches zu beachten, dass der Betroffene bei der Nutzung eines Sprachassistenten ebenso wie bei einem Telefonat, der Versendung einer E-Mail oder der Beteiligung an einem Chat aktiv Informationen aus seiner Privatsphäre offenbart, sodass auch hier ein besonderes Gefährdungspotenzial für die Privatheit dieser durch Telemedien übermittelten Informationen besteht. Dennoch lassen sich diesem Urteil des BVerfG jedenfalls Tendenzen erkennen, die einen zwischenmenschlichen Bezug in Form einer Beteiligung von mindestens zwei Menschen für den Schutz durch das Telekommunikationsgeheimnis fordern.[343] Denn das Gericht spricht im Zusammenhang mit der Eröffnung des Schutzbereiches von der *„räumlichen Distanz zwischen den Beteiligten"*[344] und einer individuellen Kommunikation und einem Kommunikationsvorgang *„zwischen Menschen"*[345]. Der gewählte Plural ließe somit auf das Erfordernis einer Kommunikation zwischen mindestens zwei Menschen schließen.

Allerdings betont das BVerfG gleichfalls, dass für den Schutz durch Art. 10 GG ein menschlich veranlasster Informationsaustausch stattfinden müsse. Bei der Informationsgewinnung durch einen IMSI-Catcher im Falle der gesprächsunabhängigen Erhebung von Standortdaten im „standby"-Modus eines Mobiltelefons, fehlt es jedoch gerade an einem solchen Austausch, der individuelle Züge aufweist.[346] Für die hier zu klärende Frage bedeutet dies jedoch, dass aus dem Beschluss folglich nicht eindeutig gefolgert werden, dass die Eröffnung des Schutzbereiches des Art. 10 GG

342 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 57 = teilweise in NJW 2007, 351 ff.

343 So *Grözinger*, Die Überwachung von Cloud-Storage, S. 79 f.

344 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 51.

345 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 57.

346 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 57; *Krüger*, ZJS 2012, 606, 610; *Harnisch/Pohlmann*, HRRS 2009, 202, 211 f.; a.A.: *Nachbaur*, NJW 2007, 335, 337; *Roggan*, KritV 2003, 76, 89 f.; *Schenke*, AöR 2000, 1, 20; *Wolter* in: SK-StPO, § 100i StPO Rn. 12.

gerade an der fehlenden Beteiligung zweier menschlicher Personen scheiterte. Ginge man davon aus, dass das Bundesverfassungsgericht die Schutzbereichseröffnung allein aufgrund des nicht menschlich veranlassten Informationsaustausches ablehnte, so erscheint es auch unter Berücksichtigung dieses Beschlusses möglich, die Nutzung eines Sprachassistenten unter den Schutz des Art. 10 GG zu fassen. Denn die Datenübertragung und damit auch die Informationsvermittlung bei der Nutzung eines Sprachassistenten ist gerade menschlich veranlasst. Ferner ist sie auch hinreichend individualisiert, da ein konkreter Betroffener Informationen preisgibt. In Anbetracht des Schutzzweckes des Art. 10 GG, der gerade dem Schutz vor der Gefahr eines Zugriffs durch staatliche Stellen auf räumlich distanzierte Nachrichtenübermittlung und der damit einhergehenden Einbuße an Privatsphäre dient,[347] könnte zu schließen sein, dass die durch eine Person veranlasste Übertragung von Daten zum Sprachassistenten durch Art. 10 GG geschützt ist. Ob das BVerfG die Kommunikation zwischen zwei Personen als zwingend erforderlich für die Gewährung des Schutzes aus Art. 10 GG erachtet, kann aus der vorliegenden Entscheidung jedenfalls nicht abschließend gefolgert werden.

(4.1.3) Surfen im Internet-Beschluss

Für eine Bestimmung der Telekommunikation i.S.d. Art. 10 GG ist darüber hinaus die oben bereits angeführte Entscheidung des BVerfG zum „Surfen im Internet" von Interesse. Die Entscheidung geht auf einen Beschluss des LG Ellwangen zurück, wonach die Überwachung der Websitennutzung durch § 100a StPO erfolgen könne. Das Landgericht stellte fest, dass es sich beim Surfen im Internet um Telekommunikation i.S.d. § 100a StPO handelt.[348] Während die Entscheidung des LG Ellwangen zunächst zur Vergleichbarkeit der Situation mit der bei der Nutzung eines Sprachassistenten im Rahmen einer technikorientierten Auslegung des Telekommunikationsbegriffes des § 100a StPO bemüht wurde, soll sie hier primär zur weiteren Klärung der Ausformung des Schutzbereichs aus Art. 10 GG herangezogen werden. Die Beschwerdeführer rügten in ihrer Beschwerdebegründung, dass das LG Ellwangen, indem es einer technikorientierten Auslegung des Telekommunikationsbegriffes gefolgt ist, verkannt habe, dass sich die Auslegung des § 100a StPO an Art. 10 GG

347 *Durner* in: Maunz/Dürig-GG, Art. 10 GG, Rn. 69.
348 LG Ellwangen, Beschl. V. 28.05.2013, Az.: 1 Qs 130/12.

orientiere müsse.[349] Für die Eröffnung des Schutzbereichs des Art. 10 GG sei nach dem Verständnis der Beschwerdeführer entscheidend, dass ein Informationsaustausch zwischen Menschen stattfinde. Bei der Informationsabfrage über das Internet finde allerdings ein bloßer Datenaustausch mit dem Netzwerk, jedoch keine zwischenmenschliche Kommunikation statt.[350] Der gesamte Vorgang der Informationsbeschaffung sei ein einseitiger Vorgang des Benutzers und daher Art. 10 GG nicht einschlägig, womit folglich auch keine Telekommunikation i.S.d. § 100a StPO vorliegen könne.[351] Ohne an dieser Stelle bereits den vielfach gezogenen Schluss von Schutzumfang auf Eingriffsermächtigung näher zu thematisieren, kann die im Anschluss an das LG Ellwangen vom BVerfG überprüfte Entscheidung dahingehend beleuchtet werden, ob das BVerfG „Surfen im Internet", der Argumentation der Beschwerdeführer folgend, unter Art. 10 GG fassen würde. Zunächst legte das Gericht unter strenger Beachtung des eigenen Prüfungsmaßstabs dar, dass die Auslegung und Anwendung strafprozessualer Normen, sofern in der fachgerichtlichen Entscheidung keine Willkür liegt oder spezifisches Verfassungsrecht verletzt wird, nicht Aufgabe des Bundesverfassungsgerichts sei.[352] Demzufolge sei die Auffassung des LG Ellwangen einem technikorientierten Telekommunikationsbegriff zu folgen nicht zu beanstanden.[353] Gleichwohl unternahm das Gericht Ausführungen zu der Frage, inwiefern das Surfen im Internet dem Schutzbereiches des Art. 10 GG unterfallen könne. Entscheidend für eine Eröffnung des Schutzbereiches streitet nach den Ausführungen des Bundesverfassungsgerichts, dass der Betroffene die Internetnutzung in dem Glauben an deren Vertraulichkeit vornahm.[354] Zudem findet im Gegensatz zum Einsatz eines IMSI-Catchers gerade nicht lediglich ein bloßer Datenaustausch statt, sondern es liegt ein konkretes Gefährdungspotential für die

349 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 16 = teilweise in NJW 2016, 3508 ff.
350 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 17 = teilweise in NJW 2016, 3508 ff.
351 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 10 = teilweise in NJW 2016, 3508 ff.
352 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 24 = teilweise in NJW 2016, 3508 ff.
353 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 24 = teilweise in NJW 2016, 3508 ff.
354 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 37 = teilweise in NJW 2016, 3508 ff.

Vertraulichkeit der Kommunikation vor.[355] Eben auf dieses Gefährdungspotential rekurrierte das Bundesverfassungsgericht bereits im Rahmen der – auch im Laufe dieser Arbeit noch relevant werdende – Entscheidung zur Beschlagnahme von E-Mails. Bereits in der damaligen Entscheidung war die spezifische Gefährdungslage aufgrund eines technisch bedingten Mangels an Beherrschbarkeit des gewählten Übermittlungsvorgangs das entscheidendes Kriterium für die Schutzbereichseröffnung des Art. 10 Abs. 1 Var. 3 GG.[356] Daher kann der Aspekt, ob der Nutzer die Daten beherrschen und ausreichende Schutzvorkehrungen treffen kann, als ein zentrales Kriterium bezüglich der Frage, ob eine telekommunikationsspezifische Gefährdungslage vorliegt, herangezogen werden.[357] Überhaupt knüpfe der Schutz durch das Telekommunikationsgeheimnis nicht an die Beteiligten einer Kommunikation, sondern an den Übermittlungsvorgang als solchen und das dabei genutzt Medium an.[358] Zuletzt stelle ein Informationsabruf im Internet auch eine körperlose Informationsübermittlung an einen individuellen Rezipienten dar.[359] Entscheidend ist allein die Individualität des Empfängers, der keinen unüberschaubaren Adressatenkreis darstellen darf.[360]

Insofern verhält sich die Entscheidung zwar auch nicht ausdrücklich zur Frage ob an einem Kommunikationsvorgang zwei Menschen beteiligt sein müssen. Sie gibt allerdings ein starkes Indiz, dass dies – sofern eine grundrechtstypische Gefährdungssituation besteht – von untergeordneter Bedeutung ist. Ferner klingt in der Entscheidung an, dass es im Lichte des Art. 10 GG nicht eines menschlichen Kommunikationspartner bedarf, solange eine Informationsabfrage auf Veranlassung des Betroffenen geschieht und dieser als Empfänger der Abfrage individualisierbar ist. Der Frage, ob ein Verhalten Telekommunikation i.S.d. Art. 10 GG darstellt, legt das BVerfG daher weniger ein personales Verständnis, sondern vielmehr ein durch Sinn und Zweck der Grundrechte als bürgerschützendes Recht geleitetes formal technisches Verständnis zu Grunde.

---

355 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 38 = teilweise in NJW 2016, 3508 ff.

356 BverfGE 124, 43, 55.

357 *Brodowski/Eisenmenger*, ZD 2014, 119, 121; *Schwabenbauer*, AöR 2012, 1, 34; *Martini* in: v. Münch/Kunig, Art. 10 GG, Rn. 76.

358 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 36 = teilweise in NJW 2016, 3508 ff.

359 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 38 = teilweise in NJW 2016, 3508 ff.

360 BverfGE 115, 166, 182; *Durner* in: Maunz/Dürig-GG, Art. 10 GG, Rn. 70.

(4.1.4) Zwischenergebnis

Die höchstrichterliche Rechtsprechung des Bundesverfassungsgerichts zeigt, dass für die Eröffnung des sachlichen Schutzbereiches nicht zwingend ein zwischenmenschlicher Informationsaustausch erforderlich ist. Vielmehr genügt es, wenn zur Nachrichtenübermittlung ein während der Übertragungsphase nicht beherrschbares Medium benutzt wird. Eine Einschränkung dahingehend, dass zwei natürliche Personen handeln müssen, ist Art. 10 GG auch im Übrigen fremd, sodass es für die Gewährleistung des Schutzgehalts gleich ist, ob eine Information lediglich an einen Server oder einen Menschen übermittelt wird. Maßgeblich ist vielmehr, dass der Vorgang auf Veranlassung des Betroffenen geschieht und dieser dabei der typischen Gefährdungslage, die mit der Nutzung eines technischen Kommunikationsmediums einhergehen, ausgesetzt ist. Dem folgend ist auch der Nutzer eines Sprachassistenten einer für Art. 10 GG typischen Gefährdungssituation ausgesetzt. Im Zuge der über die Server des Sprachassistenten durchgeführten Informationsabfrage besteht die Gefahr, dass Dritte auf diese Daten zugreifen. Diese Einschaltung des Servers in die Informationsabfrage führt dazu, dass sich die Daten nicht im ausschließlichen Herrschaftsbereich des Nutzers befinden und sie daher einem staatlichen Zugriff leichter ausgesetzt sind als eine direkte Kommunikation unter Anwesenden.[361] Ferner erfolgt die Informationsabfrage jedenfalls im klassischen Anwendungsfall auch auf Veranlassung des Nutzers, der den Sprachassistenten über das Codewort aktiviert. Der Entwicklung der Rechtsprechung folgend ist daher anzunehmen, dass diese die Nutzung eines Sprachassistenten unter Art. 10 GG fassen würde.

(4.2) Ansichten in der Literatur

(4.2.1) Multipersonale Strömung

Teilweise werden für die Schutzbereichseröffnung des Art. 10 GG zwingend zwei menschliche Kommunikationspartner gefordert.[362] Die fehlende Beteiligung einer zweiten Person bei der Nutzung eines Sprachassis-

361 Vgl. BverfGE 124, 43, 55.

362 *Grözinger*, Die Überwachung von Cloud-Storage, S. 98; *Soiné*, MMR 2015, 22, 23; *Martini* in: v. Münch/Kunig, Art. 10 GG, Rn. 73.

tenten würde diesen Vorgang hiernach nicht in den Schutzbereich der Telekommunikationsfreiheit fallen lassen.

(4.2.2) Differenzierende Ansicht

Eine differenzierende Strömung will bereits bei der Frage der Schutzbereichseröffnung des Art. 10 GG an ein materielles Kommunikationsverständnis anknüpfen.[363] Hinsichtlich der Internetnutzung sei bereits bei der Frage der Schutzbereichseröffnung des Art. 10 GG zwischen einer „kommunikativen" und einer „nicht kommunikativen" Internetnutzung zu unterscheiden.[364] Der Schutzbereich solle nur Kommunikationsdienste des Internets, wie E-Mail, Messenger-Systeme oder der Internet-Telefonie einbeziehen, während die nicht-kommunikative Nutzung des Internets, wie etwa der Besuch bestimmter Web-Seiten zur einseitigen Informationserlangung, nicht dem Schutzbereich unterfallen solle. In diesen Fällen soll vielmehr der Schutzbereich der informationellen Selbstbestimmung eröffnet sein.[365] Will man den Telekommunikationsbegriff in § 100a StPO analog zum verfassungsrechtlichen Telekommunikationsbegriff verstehen, so wäre aufgrund der dargestellten Vergleichbarkeit der Fälle des Surfens im Internet und der Nutzung eines Sprachassistenten zur Informationserlangung nach Ansicht von *Braun* und *Eschelbach* bereits der Schutzbereich des Art. 10 GG nicht eröffnet.[366] Analog hierzu bestünde dann auch keine Telekommunikation i.S.d. § 100a StPO.

(4.2.3) Unipersonale Strömung

Die wohl herrschende Ansicht innerhalb dieser Strömung erachtet es für die Schutzbereichseröffnung für ausreichend, wenn eine Person am Kom-

---

363 Insofern sind die Ausführungen durchaus vergleichbar mit einem materiellen Telekommunikationsverständnis im Rahmen des § 100a StPO, jedoch nimmt die hier angeführte Auffassung diese materiellen Einschränkungen nicht erst bei der Eingriffsermächtigung, sondern bereits auf Verfassungsebene im Rahmen des Grundrechts vor.

364 *Braun*, jurisPR-ITR 18/2013 Anm. 5; *ders*. HRRS 2013, 500, 503, *Eschelbach* in: SSW-StPO, § 100a StPO, Rn. 5.

365 *Braun*, jurisPR-ITR 18/2013 Anm. 5.

366 Vgl. *Braun*, jurisPR-ITR 18/2013 Anm. 5; *ders*. HRRS 2013, 500, 503, *Eschelbach* in: SSW-StPO, § 100a StPO, Rn. 5.

munikationsvorgang beteiligt ist. Nur so könne der bestehenden grundrechtstypischen Gefährdungslage Rechnung getragen werden, die eben auch in diesen Situationen bestehe. Daher wäre es mit dem anerkannten Grundsatz nicht in Einklang zu bringen einem unipersonal stattfindenden Vorgang den Schutz durch Art. 10 GG zu verwehren.[367] Demnach käme diese Ansicht für die Nutzung eines Sprachassistenten zur Eröffnung des Schutzbereichs aus Art. 10 GG.

(4.3) Stellungnahme

Nur durch ein formal technisches Schutzbereichsverständnis, das sich von einer strikt personalen Betrachtung des Fernmeldegeheimnisses löst und damit einhergehend einen weiten Schutzbereich garantiert, kann der Sinn und Zweck der Grundrechte in Gänze erfüllt werden. Unter Beachtung dessen, dass die technologische Entwicklung im heutigen Zeitalter eben die Nachrichtenübermittlung zwischen Menschen und Maschine ermöglicht, streitet hierfür auch die vielfach zitierte Entwicklungsoffenheit der Grundrechte.[368] Um diesem Grundsatz nachkommen zu können, muss gerade ein weites Schutzbereichsverständnis angelegt werden. Andernfalls würde in Anbetracht der Dynamisierung der verschiedensten Arten von Kommunikation, Informationsbeschaffung oder Übertragungstechniken kein hinreichender Grundrechtsschutz bestehen. Daher darf es für die Eröffnung des Schutzbereiches nicht von Belang sein, ob ein oder zwei Personen an einem Telekommunikationsvorgang beteiligt sind. Auch derjenige der eine Kommunikation mit einer technischen Maschine führt und so Informationen erhält oder die Ausführung einer Aktion befiehlt, übermittelt eine „Nachricht" mittels der Fernmeldetechnik. Entscheidend ist stets, ob sich der Nutzer durch die Verwendung der Telekommunikationstechnik in die Gefahr begibt, dass auf seine übermittelten Informationen leichter zugegriffen werden könnte.[369] In Anbetracht dessen, dass der Nutzer bei Verwendung eines Sprachassistenten zudem gerade davon ausgeht, dass seine Informationen nicht an einen menschlichen Kommunikations-

367 *Wolff* in: Hömig/Wolff-GG, Art. 10 GG, Rn. 6; *Brodowski/Eisenmenger,* ZD 2014, 119, 121; *Singelnstein*, NStZ 2012, 593, 595; *Sievers*, Der Schutz der Kommunikation im Internet, S. 106; die Schutzbedürftigkeit des Grundrechtsträger in den Vordergrund stellend auch BverfGE 124, 43, 56; BVerfG, NJW 2007, 351, 354.

368 Hierzu nur BVerfG, Urt. v. 02.03.2006, 2 BvR 2099/04; *Durner* in: Maunz/Dürig-GG, Art. 10 GG, Rn. 64.

369 BverfGE 124, 43, 55.

partner gelangen, sondern lediglich von einem technischen System beantwortet oder ausgeführt werden, steigt im Wege eines Erst-Recht-Schlusses die Vertraulichkeit dieser übermittelten Informationen. Der Schutz dieses Sachverhalts durch Art. 10 GG muss daher erst recht bestehen. Für das Erfordernis zweier Personen zur Schutzbereichseröffnung bringt vor allem *Grözinger* vor, dass in den Fällen einer nur einseitigen Telemediennutzung ein Schutz durch das IT-Grundrecht näher liege, da ein solch „einseitiger Vorgang" wesensverschieden zu den klassischen Telekommunikationsvorgängen sei.[370] Allerdings trifft *Grözinger* diese Aussage im Zusammenhang mit der Frage, ob das Ablegen von Dateien in Clouds, auf die lediglich der Nutzer selbst Zugriff hat, Kommunikation darstellen kann. Diese Situation ist nicht vergleichbar mit der Nutzung eines Sprachassistenten. Denn bei dessen Nutzung steht der kommunikative Aspekt deutlich mehr im Vordergrund. So wäre es beispielsweise für eine Dritte Person, die sich außerhalb eines Raumes aufhält, nicht sofort erkennbar, ob der Nutzer eines Sprachassistenten bloß mit einer Maschine oder einem Menschen spricht. Auch ansonsten ist die lediglich einseitige Nutzung einer Fernmeldetechnik nicht vom Schutzumfang des Art. 10 GG ausgeschlossen. Dem widerspricht auch nicht, dass das BVerfG in seiner alten Definition den Schutzbereich des Art. 10 GG derart verstand, dass hierunter der Austausch von Nachrichten, Meinungen oder Gedanken fiel. Aus dieser Definition ist keineswegs zu folgern, dass ein Austausch denklogisch nur zwischen zwei Personen möglich sei, weshalb eben auch zwei Personen für einen Kommunikationsvorgang vorhanden sein müssten.[371] Gerade das Beispiel eines Sprachassistenten zeigt, dass Nachrichten auch zwischen einer Person und einem technischen System ausgetauscht werden können. Denn der Sprachassistent reagiert jeweils individuell auf die Aussage des Nutzers, sodass dadurch durchaus ein Austausch von Nachrichten stattfindet. Ob der Nutzer eine reale Person oder einen virtuellen Assistenten zu einem bestimmten Sachverhalt befragt, hat auf das Vorliegen eines Austausches von Informationen keinen Einfluss. In die gleiche Richtung verlief bereits die Argumentation des BVerfG als dieses klarstellte, dass auch bei der Internetnutzung durch eine natürliche Person nicht ausschließlich technische Geräte miteinander kommunizieren und daher gerade nicht wie beim Einsatz „IMSI-Catchers" – lediglich ein Datenaustausch zur Sicherung

370 *Grözinger*, Die Überwachung von Cloud-Storage, S. 97.
371 So aber *Grözinger*, Die Überwachung von Cloud-Storage, S. 93.

der Betriebsbereitschaft stattfindet.[372] Sofern also auch nach dem Urteil des BVerfG zur Überwachung der Internetnutzung unter Rückgriff auf das Urteil des BVerfG zum Einsatz eines IMSI-Catchers gefolgert wird, dass das BVerfG zwingend zwei Personen für einen Telekommunikationsvorgang im Rahmen des Art. 10 GG für erforderlich halten würde, fußt dies auf einer unvollständigen Auswertung der höchstrichterlichen Rechtsprechung. Mittlerweile wird der Schutzbereich zudem durch das BVerfG dahingehend modifiziert, dass bereits die unkörperliche Informationsübermittlung an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs schützenswert ist.[373] Vom Begriff des klassischen Austausches hat sich auch diese Definition hin zur Übermittlung entwickelt. Jedenfalls eine Übermittlung von Informationen findet aber auch statt wenn ein technisches Gerät einem Menschen Informationen zukommen lässt. Für eine Informationsübermittlung sind daher keine zwei Menschen erforderlich.

Für die differenzierende Auffassung *Brauns* und *Eschelbachs* ergeben sich aus Art. 10 GG keine Anhaltspunkte, um bereits auf der Stufe der Schutzbereichseröffnung zwischen einer kommunikativen und einer nicht kommunikativen Internetnutzung zu unterscheiden. Vielmehr folgt aus dem Wortlaut „Fernmeldegeheimnis", dass sobald sich eine Person der Fernmeldetechnik bedient, der hierdurch übermittelte Inhalt „geheim" bleiben soll und daher durch Art. 10 GG geschützt ist, gleich ob es sich dabei um eine kommunikative oder nicht-kommunikative Internetnutzung handelt. Um den Wortlaut aus Art. 10 GG[374] jedoch nicht überzustrapazieren, kann der bloße Datenaustausch zwischen Maschinen, der gerade nicht menschlich veranlasst wurde, nicht unter den Schutz des Art. 10 GG fallen.[375] Dies würde den gesetzgeberischen Willen, mit Grundrechten stets die menschlich veranlasste Kommunikation zu schützen, missachten.

372 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 38 = teilweise in NJW 2016, 3508 ff.

373 BVerfGE 115, 166, 182; BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 33 = teilweise in NJW 2016, 3508 ff.

374 Dieser spricht streng genommen nur vom sog. Fernmeldegeheimnis. Allerdings ist zu Recht allgemein anerkannt, dass hierunter auch das Telekommunikationsgeheimnis fällt, vgl. nur BVerfG, NJW 2002, 3619, 3620. Auch in der Literatur ist umfassend nicht mehr von dem Fernmeldegeheimnis, sondern dem Telekommunikationsgeheimnis die Rede, vgl. m.w.N *Ogorek* in: BeckOK-GG, Art. 10 GG, Rn. 35.

375 A.A. wohl *Gähler*, HRRS 2016, 340, 343.

Vielmehr würde dann ein bloßes, dem Informationsaustausch dienliches maschinelles System geschützt.[376]

Zuletzt wird in der Literatur vorgebracht, dass sich die Entwicklungsoffenheit der Grundrechte lediglich auf die neuartigen technischen Formen der Übertragung beziehe, nicht aber auf die Frage, was Kommunikation im Sinne des Kommunikationsgeheimnisses darstellt.[377] Eine solche isolierte Betrachtung kann jedoch nicht trennscharf vorgenommen werden. Dies zeigt sich bereits am Beispiel der Mailbox oder des E-Mail-Verkehrs, deren Nutzung unter das Telekommunikationsgeheimnis fällt[378].[379] Mit der technischen Schaffung der Möglichkeit eine Nachricht zu speichern und später abzurufen, entstand eine neue technische Form der Nachrichtenübertragung, die aufgrund der Entwicklungsoffenheit des Grundrechts in den Schutzbereich fällt. Gleichsam entwickelte sich dadurch aber auch das Kommunikationsverständnis als solches weiter. Unter Kommunikation fällt nicht mehr nur der unmittelbare Austausch von Informationen wie in einem Telefongespräch, sondern auch die Speicherung und der zeitlich verzögerte Abruf einer Nachricht.[380] Insbesondere entschied das BVerfG in der Entscheidung hinsichtlich der Speicherung von E-Mails, dass der E-Mail-Verkehr gerade auch deswegen unter den Schutz des Art. 10 GG fallen, da der Nutzer während die E-Mail beim Provider gespeichert ist, keine Möglichkeit hat, diese gegen unbefugten Zugriff durch den Staat oder den Provider selbst zu schützen.[381] Aus diesem Mangel an Beherrschbarkeit folgt wiederum die grundrechtstypische Gefährdungssituation, die eine besondere Schutzbedürftigkeit durch das Fernmeldegeheimnis erfordere.[382] Um einen hinreichenden Schutz in dieser Gefährdungssituation auch in neu entstehenden Fällen – wie dem der Nutzung eines Sprachassistenten zu gewährleisten – ist es daher erforderlich, auch den verfassungsrechtlichen Kommunikationsbegriff als solchen ebenso wie die Frage nach technischen Formen der Nachrichtenübermittlung im Wandel

376 So bzgl. der Nichteröffnung des Schutzbereichs aus Art. 10 GG hinsichtlich solcher Vorgänge ohne menschliche Beteiligung auch *Grözinger*, Die Überwachung von Cloud-Storage, S. 93.

377 *Grözinge*r, Die Überwachung von Cloud-Storage, S. 94.

378 *Durner* in: Maunz/Dürig-GG, Art. 10, Rn. 107.

379 Hinsichtlich der E-Mail-Nutzung fällt jedenfalls der Abschnitt solange die E-Mail auf dem Server des Providers gespeichert und noch nicht abgerufen wurde unter den Schutz des Art. 10 GG.

380 BVerfGE 124, 43, 55.

381 BVerfGE 124, 43, 55.

382 BVerfGE 124, 43, 55.

der Zeit entwicklungsoffen zu betrachten. Nur dadurch kann der Schutzgehalt aus Art. 10 GG vollumfänglich gewahrt werden.

(5) Zwischenergebnis

Kommunikation im Sinne von Art. 10 GG setzt somit keine Beteiligung zweier Personen voraus. Die Nutzung eines Sprachassistenten fällt demnach unter den Schutzbereich des Art. 10 GG. Sofern der Telekommunikationsbegriff aus § 100a StPO analog zu Art. 10 GG ausgelegt werden soll, handelt es sich daher bei der Sprachassistentennutzung um Telekommunikation i.S.d. § 100a StPO.

dd) Strafprozessualer Telekommunikationsbegriff

Den verschiedenen Ausgestaltungen eines strafprozessualen Telekommunikationsbegriffs folgend, stellt sich ebenfalls die Frage, inwiefern während des Übertragungsweges zum Server von Kommunikation gesprochen werden kann. Sofern eine soziale Interaktion gefordert wird, könnte diese im hiesigen Beispiel lediglich mit dem Server erfolgen. Dies erscheint jedoch befremdlich. Soziale Interaktion beinhaltet bereits nach dem allgemeinen Wortsinn eine bewusst ablaufende zwischenmenschliche Interaktion. Daher kann dem Telekommunikationsbegriffsverständnis *Hiéramentes* folgend, bei der Nutzung eines Sprachassistenten während der Übertragung nicht von Telekommunikation i.S.d. § 100a StPO gesprochen werden. Dieses Ergebnis untermauern auch die Ausführungen *Hiéramentes*, der das Surfen oder Googeln im Internet zur Informationsgewinnung eher einem Selbstgespräch- oder Tagebucheintrag zuordnen will, hierin aber jedenfalls keine Kommunikation i.S.d. § 100a StPO sieht.[383] Die Konstellation der Nutzung eines Sprachassistenten ist mit dem bloßen Surfen im Internet durchaus vergleichbar. In beiden Konstellationen erhofft sich der Nutzer Antworten oder Informationen auf Fragen und dergleichen. Auch wer mit *Wicker* einen Mitteilungswillen in den Telekommunikationsbegriff nach § 100a StPO hineinlesen will[384], kommt zu keinem anderen Ergebnis. Im Unterschied zur klassischen Kommunikation bei der welcher sich der Äußernde per E-Mail, Telefonat oder Chat seinem Gegenüber

383 *Hiéramente*, HRRS 2016, 448, 451.
384 *Wicker*, Cloud Computing und staatlicher Strafanspruch, S. 380 f.

mitzuteilen vermag, ist bei der Nutzung eines Sprachassistenten primäres Hauptziel nicht die zwischenmenschliche Kommunikation gepaart mit einem Mitteilungswillen, sondern die bloße Informationsgewinnung. Genau genommen kann daher nicht von einem Mitteilungswillen, sondern (lediglich) von einem Informationswillen gesprochen werden. Es kommt dem Nutzer hier gerade nicht darauf an, dem Server etwas um der Mitteilung willen mitzuteilen, sondern lediglich, um eine korrekte Antwort auf die gestellte Frage zu erhalten.

c) Auf der Cloud des Diensteanbieters

Es bleibt zu klären, ob ein Zugriff über § 100a StPO auch noch möglich ist, wenn sich die Daten auf der Cloud des Dienstleistungsanbieters befinden.

aa) Technischer Kommunikationsbegriff

Aus Sicht des technischen Kommunikationsbegriffes ist festzuhalten, dass die Audioaufzeichnungen nach deren Bearbeitung auf der Cloud des Diensteanbieters ruhen. Ein „Aussenden, Übermitteln, oder Empfangen", liegt wie von § 22 Nr. 3 TKG gefordert nicht mehr vor. Somit würde nach dem rein technischen Telekommunikationsbegriff in diesem Stadium keine Telekommunikation i.S.d. § 100a StPO mehr vorliegen.

bb) Technikorientierter Telekommunikationsbegriff

Anders könnte diese Frage zu beantworten sein, sofern der technikorientierten Auslegung gefolgt werden soll. Bei konsequenter Vorgehensweise und Beachtung des Umstandes, dass diese Sichtweise die rein technikorientierte Sichtweise weiter einschränken soll, kann, wenn schon nach der rein technischen Ansicht in diesem Stadium keine Telekommunikation i.S.d. § 100a StPO mehr vorliegt, nach technikorientierten Telekommunikationsbegriff erst recht keine Telekommunikation vorliegen. Widersprüchlich hierzu ist jedoch die Entscheidung eines Ermittlungsrichters, des dieser Ansicht grundsätzlich zugewandten Bundesgerichtshofs. Der Ermittlungsrichter am BGH entschied, dass auch auf bereits auf einer Mailbox ruhende Nachrichten noch mittels § 100a StPO zugegriffen wer-

den könnte.[385] In einer späteren Entscheidung zur Online-Durchsuchung und dem Zugriff auf die auf einem Computer gespeicherten Daten, stellte der BGH ohne Begründung fest, dass § 100a StPO nicht als Ermächtigungsgrundlage in Frage komme.[386] Auf die frühere Entscheidung des Ermittlungsrichters wurde lediglich derart hingewiesen, dass diese den einmaligen heimlichen Zugriff auf eine passwortgeschützte Mailbox unter Heranziehung des § 100a StPO legitimierte.[387] Aus der Art und Weise der Verweisung lässt sich jedoch schlussfolgern, dass der Bundesgerichtshof diese Entscheidung heute so nicht mehr treffen würde. Schließlich wird in der Begründung der neueren BGH-Entscheidung ausgeführt, dass der damalige Ermittlungsrichter einen ähnlichen Sachverhalt „anders" bewertet habe.[388] Diese Formulierung wird im juristischen Sprachgebrauch in der Regel dann benutzt, wenn auf eine andere abweichende Meinung hingewiesen werden soll. Zudem zitiert der Bundesgerichtshof in seinen Urteilsbegründungen, sofern er seine Zustimmung zu einem früheren Urteil zum Ausdruck bringen will und sich hieran anschließt in der Regel mit Worten „so auch" oder „zuvor bereits".[389] Daher dürfte die Entscheidung des Ermittlungsrichters als einmalige Fehlinterpretation zu werten sein und der Bundesgerichtshof würde in Einklang mit der technikorientierten Auffassung zum Ergebnis kommen, dass die auf den Server des Sprachassistenten gespeicherten und dort ruhenden Informationen keine Telekommunikation i.S.d. § 100a StPO darstellen.

cc) Grundrechtsanaloger Telekommunikationsbegriff

Aus Sicht der grundrechtsanalogen Ansicht ist nicht entscheidend, ob die Daten noch in Bewegung sind oder bereits auf dem Speichermedium ruhen. Ein dynamischer Übermittlungsvorgang ist nicht notwendige Voraussetzung für die Schutzbereichseröffnung, sofern die von der Übermittlung ausgehende grundrechtstypische Gefährdungslage auch bei ruhenden Daten weiter fortbesteht.[390] Eine gegenteilige Schlussfolgerung lässt sich ferner auch nicht aus der Entscheidung zur "Online-Durchsuchung" des

385 BGH, NStZ 1997, 247.
386 BGH, MMR 2007, 237, 239.
387 BGH, MMR 2007, 237, 239.
388 BGH, MMR 2007, 237, 239.
389 Vgl. nur BGH, MMR 2015, 839, 840; BGH, NStZ 2016, 741, 743.
390 BverfGE 124, 43, 55 f.

BVerfG ableiten. Zwar betont das Gericht dort mehrfach, dass Art. 10 Abs. 1 GG die Inhalte und Umstände des "laufenden" Kommunikationsvorgangs umfasse.[391] Dagegen muss im Falle der virtuellen Speicherung einer Audioaufzeichnung berücksichtigt werden, dass die Beendigung eines laufenden Kommunikationsvorgangs nicht ebenso trennscharf bestimmt werden kann, wie dies beispielsweise im Rahmen einer Postsendung oder eines Telefonanrufes möglich ist. Während in den dortigen Fällen der Telekommunikationsvorgang mit dem Verlauten der Nachrichten am Telefonhörer als Endgerät oder mit Übergabe der Postsendung abgeschlossen ist, bleibt bei der virtuellen Speicherung der Audioaufzeichnung das dem Telekommunikationsvorgang immanente Risiko eines vereinfacht durchführbareren Zugriff Dritter weiter fortbestehen. Daher erscheint es folgerichtig, dass das Gericht einem weiteren Kriterium zur Bejahung oder Verneinung der Schutzbereichseröffnung des Art. 10 GG eine wohl noch gewichtigere Bedeutung beimisst. Die nach Abschluss eines Kommunikationsvorgangs vorhandenen Daten werden durch das Gericht nicht primär vom Schutzbereich des Art. 10 GG ausgenommen, weil diese nicht mehr in Bewegung sind, sondern weil diese im Herrschaftsbereich eines Kommunikationsteilnehmers gespeichert sind, der seinerseits auch eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff hätte treffen können.[392] Ausschlaggebend ist daher nicht, ob sich die Daten in einem laufenden Übermittlungsvorgang befinden, sondern vielmehr, ob der Nutzer weiterhin über diese Daten herrscht und er ausreichende Schutzvorkehrungen gegen eine unbefugte Verwendung treffen kann.[393] Daher können Cloud-Speicher auch nicht mit lokalen Speichermedien gleichgesetzt werden.[394] Zutreffend ist diese Sichtweise, da Cloud-Speicher – ähnlich wie E-Mail-Server – durch den Dienstleistungsanbieter fremdbeherrscht sind.[395] Dem Dienstleistungsanbieter sind die Daten zum einen technisch zugänglich und zum anderen kommt ihm die Hoheitsmacht zu, dem Nutzer den Zugriff auf die gespeicherten Daten vollständig vorent-

391 BverfGE 120, 274, 308 ff.; BverfGE 120, 274, 340.
392 BverfGE 120, 274, 308; BverfGE 124, 43, 55 f.
393 So auch *Gähler*, HRRS 2016, 340, 345; *Gersdorf* in: BeckOK-InfoMedienR, Art. 10 GG, Rn. 17 f.; *Brodowski/Eisenmenger*, ZD 2014, 119, 121; *Schwabenbauer*, AöR 2012, 1, 34.
394 Vgl. BverfGE 124, 43, 56.
395 BGH, NJW 2021, 1252, 1254; *Gersdorf* in: BeckOK-InfoMedienR, Art. 10 GG, Rn. 18.

halten zu können.[396] Dadurch wird auch der grundsätzliche Unterschied zur klassischen Online-Durchsuchung deutlich, bei der die Überwachung eines bestimmten Systems, das sich in der Herrschaftssphäre des Betroffenen befindet, im Vordergrund steht. Eine solche Konstellation lag auch der Entscheidung des BVerfG zur Online-Durchsuchung zugrunde, da die Online-Durchsuchung den Zugriff auf ein Zielsystem ermöglichen sollte, das sich in der Herrschaftssphäre des Nutzers befand. Das BVerfG legte seinen Überlegungen zur nicht vorhandenen Einschlägigkeit des Art. 10 GG daher ausschließlich die Situation zugrunde in der sich das Zielgerät im physischen Herrschaftsbereich des Nutzers befand, jedoch gerade nicht die Situation eines räumlich getrennten Cloud-Servers.[397] Auf einen räumlich getrennten Server bezog sich dagegen der Zugriff der Strafverfolgungsbehörden, mit welchem sich das BVerfG in der IMAP-Entscheidung befasste. In dieser Entscheidung hielt das BVerfG fest, dass die Beschlagnahme von E-Mails aus einem E-Mail-Postfach, auf das der Nutzer nur über eine Internetverbindung zugreifen kann, an Art. 10 GG zu messen ist.[398] Die beschlagnahmten Daten befinden sich hier gerade nicht im Herrschaftsbereich des Nutzers, sondern ruhen fremdbeherrscht auf den Servern des Dienstleistungsanbieters.[399] Insofern stehen die Entscheidungen des BVerfG zur Online-Durchsuchung und zur E-Mail Beschlagnahme hinsichtlich Art. 10 GG auch nicht in Widerspruch, sondern verdeutlichen vielmehr, dass die vorhandene Herrschaftsmacht des Nutzers über die Daten das entscheidende Kriterium für die Einschlägigkeit des Art. 10 GG darstellt. Folgerichtig ist der Schutzbereich des Art. 10 GG nur im Fall der E-Mail Beschlagnahme von einem fremden Server, nicht aber im Falle der Online-Durchsuchung eines physischen Endgeräts im Sinne eines lokalen Speichermediums eröffnet.

Folgt man innerhalb dieser Strömung der zutreffenden Ansicht, dass für die Schutzbereichseröffnung eine Person ausreichend ist, so unterfällt der Cloud-Speicher auch dann dem Schutzbereich des Art. 10 GG[400], wenn die Daten bereits auf dem Server des Sprachassistenten ruhen. Hinsichtlich

396 *Gersdorf* in: BeckOK-InfoMedienR, Art. 10 GG, Rn. 18; *Herrmann/Soiné*, NJW 2011, 2922, 2923; *Wicker*, DSRITB 2013, 981, 988.

397 So auch *Brodowski/Eisenmenger*, ZD 2014, 119, 121; *Gähler*, HRRS 2016, 340 346.

398 BverfGE 124, 43, 55 f. Dieser Maßstab gilt unabhängig davon, ob der Zugriff auf E-Mails im Rahmen des § 100a StPO oder im Rahmen anderer Ermächtigungsgrundlagen, wie beispielsweise § 94 StPO erfolgt, vgl. BverfGE 124, 43, 58 f.

399 BverfGE 124, 43, 55 f.

400 *Brodowski/Eisenmenger*, ZD 2014, 119, 121; *Gaede*, StV 2009, 96, 97.

§ 100a StPO würde dies bedeuten, dass sofern neben dem Merkmal der Telekommunikation auch die weiteren Voraussetzungen vorliegen, mittels dieser Norm auf die gespeicherten Daten zugegriffen werden könnte.[401]

dd) Strafprozessualer Telekommunikationsbegriff

Nach dem genuin strafprozessual bestimmten Telekommunikationsbegriff liegt bei einem Zugriff auf den Server keine Telekommunikation mehr vor. Weder findet in diesem Stadium eine soziale Interaktion statt, noch liegt bei Zugrundelegung dessen, dass die Dienstleister alte Sprachnachrichten abspeichern, um die Qualität der Spracherkennung zu erhöhen, ein Mitteilungswillen des Nutzers vor.

d) Zwischenergebnis

Vor der internetbasierten Übertragung der Audioaufzeichnungen zum Sprachassistenten scheidet ein Zugriff unter Heranziehung des § 100a StPO nach allen Ansichten aus. Hinsichtlich des Stadiums während des Übermittlungsvorgangs an die Server des Sprachassistenten bleibt festzuhalten, dass sowohl die rein technische Strömung als auch die lediglich technikorientierte Auffassung das Vorliegen eines Telekommunikationsvorgangs bejahen. Im Lager der grundrechtsanalogen Auffassung, die den Telekommunikationsbegriff in § 100a StPO grundrechtsanalog zu Art. 10 GG auslegen will, kommen die unipersonale sowie die differenzierende Auffassung aufgrund einer restriktiven Schutzbereichsauffassung

401 So vgl. BGH, NJW 2021, 1252, 1554. Äußerst kritisch zu dieser Begründung, vgl. *Grözinger*, NStZ 2021, 358 f.; *Hiéramente*, WiJ 2021, 19, 21 f.; *Trüg*, JZ 2021, 560, 564 f., die mit guten Argumenten darauf hinweisen, dass ein in Zugriff auf Datenbestände, die vor Anordnung einer Telekommunikationsüberwachung entstanden sind, nach § 100a Abs. 1 S. 1 StPO – unabhängig von dem Vorliegen von Telekommunikation – unzulässig ist. Denn eine Überwachung im Sinne des § 100a StPO könne bereits – nach dem Wortsinn – nur bei heimlicher Kenntnisnahme des Inhalts einer *laufenden* Kommunikation vorliegen. Hierfür spricht auch ein systematischer Vergleich mit den §§ 100a, 100b StPO. § 100b StPO, der von Online-Durchsuchung spricht, schließt gerade auch in der Vergangenheit generierte und damit ruhende Datenbestände mit ein. Für § 100c StPO – der wie § 100a Abs. 1 S. 1 StPO von Überwachung spricht - ist unumstrittenes Verständnis, dass denklogisch nur laufende Kommunikation überwacht werden kann.

nicht zu dessen Eröffnung, womit keine Telekommunikation vorläge. Die wohl herrschende Ansicht in diesem Lager bejaht jedoch zurecht auch bei nur einer involvierten Person die Eröffnung des Schutzbereiches, womit auch Telekommunikation i.S.d. § 100a StPO vorläge. Aus einer eigenständigen strafprozessualen Auslegung des Telekommunikationsbegriffes folgt, dass bei der Nutzung eines Sprachassistenten während des Übermittlungsvorgangs an die Server keine Telekommunikation i.S.d. § 100a StPO vorliegt.[402] Sobald die Daten auf dem Server des Sprachassistenten ruhen, verneinen sämtliche Ansichten, mit Ausnahme der unipersonalen Strömung, die den Schutzbereich des Art. 10 GG auch in diesem Fall für eröffnet erachten würde, das Vorliegen von Telekommunikation im Sinne des § 100a StPO.

e) Stellungnahme

Es bleibt die Frage, welcher Strömung zur Bestimmung des Telekommunikationsbegriffes in § 100a StPO der Vorzug zu geben ist.

aa) Kritik an den technischen Auffassungen

Den technischen Auffassungen ist entgegenzuhalten, dass es keineswegs unproblematisch erscheint, § 3 des TKG zur näheren Auslegung des § 100a StPO heranzuziehen. Dies gründet zum einen auf den divergierenden Normzwecken. Während die Eingriffsbefugnisse des TKG lediglich einen Eingriff in das Fernmeldegeheimnis aus Art. 10 GG gestatten, erlaubt das strafprozessuale Pendant hierzu auch solche in das aus dem allgemeine Persönlichkeitsrecht des Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG entstammende Recht auf informationelle Selbstbestimmung.[403] Das extensive Verständnis des § 3 TKG für die Leseart des § 100a StPO zu Grunde gelegt, würde daher den grundrechtlich durch Art. 2 Abs. 1 i.V.m. Art. 1 GG garantierten Schutz ohne Not einschränken.[404] Zum anderen verweist

402 Anders zu beurteilen sind Fälle in denen der Smart Speaker lediglich als zwischengeschaltetes Gerät verwendet wird. Daher könnte unproblematisch die Telekommunikation nach § 100a StPO überwacht werden, sofern über den Smart Speaker ein Telefonat geführt wird.

403 *Hauck* in: LR-StPO, § 100a StPO, Rn. 35; *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 24.

404 *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 24.

§ 100a StPO im Unterschied zu beispielsweise § 100g Abs. 1 S. 1 StPO gerade nicht ausdrücklich auf das TKG. Sofern der Gesetzgeber auch im Rahmen des § 100a StPO eine Heranziehung der im TKG normierten Legaldefinition gewollte hätte, hätte er auch in § 100a StPO eine entsprechende Verweisung verankert.[405] Hinzu kommt, dass das TKG nach Sinn und Zweck ein intaktes Telekommunikationswesen garantieren soll, vgl. § 1 TKG[406], wohingegen Zweck des § 100a StPO die Beweisgewinnung zur Wahrheitsfindung ist. Im Unterschied zur StPO sind die Begrifflichkeiten des TKG offensichtlich technikorientiert; mit der Wahrung der öffentlichen Sicherheit und dem Schutz der Gesellschaft, dem die StPO dient, hat das TKG keine Berührungspunkte.[407] Gegen einen Rückgriff auf die Normen des TKG spricht ferner die Existenz des § 99 StPO, der zeigt, dass zumindest einzelne Telekommunikationsformen eigenständigen Ermächtigungsgrundlagen unterfallen und daher nicht unter § 100a StPO gefasst werden sollen.[408] Durch den Versuch, mittels der Definition aus dem TKG auch die Voraussetzung in § 100a StPO mit Leben zu füllen, wird einmal mehr deutlich, dass es in der juristischen Praxis keine Seltenheit darstellt, die Auslegung eines Wortes, unterschiedliche Regelungszusammenhänge ignorierend, durch Bezugnahme auf Begriffsbildungen aus fremden Normen auszugestalten.[409] Diese Vorgehensweise ist methodisch stark zu kritisieren und kann deswegen nicht der Maßstab zur Auslegung des § 100a StPO darstellen.

Gegen ein rein technisches und damit sehr extensives Verständnis des Telekommunikationsbegriffes, welches dazu führen würde, dass auch der bloße Datentransfer zwischen Maschinen unter diesen Begriff zu subsumieren wäre, bestehen zudem bereits in Anbetracht des Wortsinns bzw. dem allgemeinen Sprachverständnis des Begriffes „Kommunikation" Bedenken.[410] Als Mindestvoraussetzung bedarf Kommunikation als Form der Verständigung die menschliche Veranlassung. Der bloße Datenaustausch zwischen elektronischen Geräten kann mit dem allgemeinem Sprachgebrauch nicht derart vereinbart werden, dass darunter eine Form der

405 So bereits *Grözinger,* Die Überwachung von Cloud-Storage, S. 207; *Günther* in: MüKo-StPO, § 100a StPO, Rn. 33.
406 *Eisenberg/Nischan*, JZ 1997, 74, 77.
407 *Günther* in: MüKo-StPO, § 100a StPO, Rn. 33.
408 *Gercke,* Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, S. 94 f.
409 So auch *Demko*, NStZ 2004, 57, 60.
410 A.A.: *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 6.

kommunikativen Verständigung verstanden werden könnte.[411] Es kann wenn ausschließlich technische Geräte miteinander in Verbindung stehen und es an einem menschlich veranlassten auf Kommunikationsinhalte bezogenen Informationsaustausch fehlt, daher keine Kommunikation i.S.d. § 100a StPO vorliegen.[412]

Selbst das LG Ellwangen, das den zur Nutzung eines Sprachassistenten ähnlich gelagerten Fall des Abrufens von Websites als Telekommunikation einstufte, dürfte hiervon nicht restlos überzeugt gewesen sein. Anders sind die Ausführungen der Kammer, wonach eine Subsumtion unter § 100a StPO auch erforderlich gewesen sei, um den Bürger zu schützen[413], nicht zu verstehen. Es wäre „fatal"[414] gewesen, wenn auf das Surfen im Internet ansonsten über die Generalklausel des § 161 StPO zugegriffen werden könnte. Dem Gericht ist insofern zuzustimmen, dass ein solches Verhalten keine schutzlose öffentliche Kommunikation darstellen darf. Die Schlussfolgerung des Gerichts dieses Problem dadurch zu lösen, das entsprechende Verhalten unter § 100a StPO zu subsumieren, ist jedoch nicht überzeugend. Denn selbst sofern § 100a StPO für nicht einschlägig befunden worden wäre, würde dies nicht bedeuten, dass auf eine spezielle Ermächtigungsgrundlage verzichtet werden kann und der Grundrechtseingriff auf die Generalklausel des § 161 StPO gestützt werden kann. Dies wäre nur dann möglich, wenn es sich bei den auf Grundlage des § 161 StPO erfolgten Grundrechtseingriff um einen nur wenig grundrechtsintensiven Eingriffe handeln würde.[415] Sowohl bei der Sichtung abgerufener Websites als auch bei dem Zugriff auf die durch Sprachassistenten vernommenen Aussagen handelt es sich allerdings um Tätigkeiten, die Einblicke in Handlungen geben, die der Betroffene im Schein absoluter Privatheit vornimmt. Solche Eingriffe in die Privatsphäre sind nicht vergleichbar mit dem kurzzeitigen Einsatz eines V-Mannes oder einer kurzzeitigen Observation, die immer wieder auf die Generalklausel gestützt werden.[416] Bei diesen Maßnahmen wird der Betroffene nicht in privaten Rückzugsräumen überwacht, sondern erst nachdem er sich in die Öffentlichkeit

411 Bernsmann, NStZ 2002, 103, 104.
412 BVerfG, MMR 2006, 805, 807.
413 LG Ellwangen, Beschluss v. 28.05.2013, Az.: 1 Qs 130/12.
414 LG Ellwangen, Beschluss v. 28.05.2013, Az.: 1 Qs 130/12.
415 *Kölbel* in: MüKo-StPO, § 161 StPO, Rn. 9; *Grießbaum* in: KK-StPO, § 161 StPO, Rn. 1.
416 Solche Maßnahmen können auf die Ermittlungsgeneralklausel, § 161 StPO, gestützt werden, vgl. *Grießbaum* in: KK-StPO, § 161 StPO, Rn. 1; *Sackreuther* in: BeckOK-StPO, § 161 StPO, Rn. 11.

begeben hat oder im Falle des Einsatzes eines V-Mannes nachdem sich der Betroffene freiwillig einer ihm Unbekannten Person offenbart hat. Die Eingriffsintensität ist daher deutlich geringer. Die richtige Schlussfolgerung des LG Ellwangen wäre daher gewesen, das Abrufen der Websites unter Heranziehung des § 100a StPO zu verbieten und sodann weitere mögliche Ermächtigungsgrundlagen der §§ 100a ff. StPO zu prüfen. Sofern keine weitere Ermächtigungsgrundlage als einschlägig befunden worden wäre, hätte der erfolgte Grundrechtseingriff aufgrund eines Verstoßes gegen den Gesetzesvorbehalt als rechtswidrig beurteilt werden müssen.

bb) Kritik an der grundrechtsanalogen Auffassung

Einem grundrechtsanalogen Verständnis des § 100a StPO ist kritisch entgegenzuhalten, dass von der Reichweite des Grundrechtsschutzes aus Art. 10 GG nicht auf die Reichweite einer grundrechtstangierenden Ermächtigungsgrundlage geschlossen werden darf.[417] Würde bei der Auslegung des einfachen Gesetzes lediglich auf den grundrechtlichen Schutzbereich zurückgegriffen, würde der Grundrechtsschutz ausgehöhlt. Sofern also eine Ermächtigungsgrundlage, auf den ersten Blick um des Grundrechtsschutzes Willen, grundrechtsanalog extensiv ausgelegt wird, führt dies letztlich die Schutzfunktion der Grundrechte ad absurdum.[418] Während Grundrechte gerade nicht den Staat berechtigen, sondern dessen Bürger schützen sollen, stellt § 100a StPO eine Berechtigung für den Staat dar, in die Rechte seiner Bürger verfassungsgemäß eingreifen zu können. Will man nun trotz dieses diametralen Unterschieds die dem Staat einfach gesetzlich zugesprochenen Eingriffsbefugnisse aus dem Schutzinhalt, den die Verfassung dem Bürger gerade zu dessen Schutz zuerkennt, ableiten, verfängt sich dies in einem Zirkelschluss zu Lasten des Bürgers. Dessen verfassungsrechtlich durch Art. 10 GG garantiertes Schutzniveau würde dadurch leerlaufen, dass dem Staat durch den inhaltlichen Gleichlauf zwischen Schutzniveau und Eingriffsermächtigung solch weite Eingriffsbefugnisse zukämen, dass der weite Schutzbereich wertlos erscheinen würde[419] Dass für einen rechtmäßigen staatlichen Eingriff dabei – wie auch im Falle

417 So auch *Hilgendorf/Valerius*, Internetstrafrecht, Rn. 783; *Roggan*, KritV 2003, 76, 80 und 89; *Grözinger, NStZ 2021, 358*.

418 *Bernsmann*, NStZ 2002, 103, 103; *Bernsmann/Jansen*, StV 1999, 591, 591; *Gercke*, GA 2012, 474, 488; *Hiéramente* WiJ 2021, 19, 21.

419 Zutreffend auch *Hiéramente/Fenina*, StraFo 2015, 365, 371.

des § 100a StPO – noch weitere tatbestandliche Voraussetzungen vorliegen müssen, vermag hieran nichts zu ändern.[420] Denn über das Vorliegen dieser weiteren Voraussetzungen ist stets losgelöst von der Frage zu entscheiden, ob das Tatbestandsmerkmal der Telekommunikation im konkreten Einzelfall gegeben ist. Ein Zusammenhang, dass sofern Art. 10 GG tangiert ist, auch das Tatbestandsmerkmal der Telekommunikation in § 100a StPO erfüllt ist, ist dem Gesetz fremd. Der Inhalt der Ermächtigungsgrundlage kann daher gerade nicht durch den Schutzbereich des Grundrechts bestimmt werden, in welches ein Eingriff unter Heranziehung eben dieser Ermächtigungsgrundlage legitimiert werden soll.[421] Insofern sind das den Bürger schützende Grundrecht und die den Staat berechtigende Ermächtigung strikt zu trennen. Wenn das BVerfG betont, dass das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG entwicklungsoffen ist und auch neuartige Übertragungstechniken umfassen soll,[422] so bedeutet das gerade nicht, dass der Begriff der Telekommunikation im Rahmen des § 100a StPO synonym hierzu auszulegen ist, sondern lediglich ebenso – aber stets in Anbetracht seines strafprozessualen Zweckes – entwicklungsoffen ist[423]. Insbesondere ist es nicht widersprüchlich Art. 10 GG entwicklungsoffen auszulegen, während dies für § 100a StPO restriktiver gehandhabt wird. Dabei ist unstreitig, dass § 100a StPO dem technischen Fortschritt dergestalt Rechnung tragen muss, dass neben dem klassischen Telefongespräch auch neuere Kommunikationsformen wie SMS, E-Mails, oder Chatnachrichten mittels § 100a StPO überwacht werden dürfen. Dieser Wechsel des Kommunikationsmediums ändert jedoch nichts an der Zielrichtung des § 100a StPO und seiner restriktiveren Auslegung im Lichte seiner selbst.[424] Es ist einmal mehr zu beachten, dass Art. 10 GG dem Schutz der Bürger dient[425] und, um dem verfassungsrechtlichen Schutzauftrag nachzukommen, eben dieser verfassungsrechtlich garantierte Schutz im Gleichschritt mit der technischen Entwicklung ausgeweitet werden muss. Hierfür sprechen nicht zuletzt auch praktische Erwägungen. Denn andernfalls müsste für neue Entwicklungen das Grundgesetz permanent geändert oder modifiziert werden. Zudem wäre der Bürger bei neuen Entwicklungen bei deren Nutzung der Bürger vor staatlichem Zugriff geschützt werden

420 A.A. *Wölm*, Schutz der Internetkommunikation und heimliche Internetaufklärung, S. 244.
421 *Wolter/Greco* in: SK-StPO, § 100a StPO, Rn. 13.
422 BVerfG NJW 2006, 976, 978.
423 A.A. *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 20.
424 Zutreffend *Hiéramente/Fenina*, StraFo 2015, 365, 370, m.w.N.
425 *Schoch*, Jura 2011, 194, 195.

muss, bis zur Schaffung eines neuen Grundrechts schutzlos gestellt. Bei den Eingriffsermächtigungen der StPO handelt es sich jedoch um formelle Gesetze. Formellen Gesetze ist es seit jeher immanent, dass sie durch zahlreiche Modifizierung ständig an die Entwicklung angepasst oder gar neu geschaffen werden.[426] Letzteres zeigt nicht zuletzt die Existenz der §§ 100a, 100b, 100c StPO selbst.

Auch wenn Art. 10 GG nach den Ausführungen des BVerfG den „verfassungsrechtlichen Maßstab"[427] für die Eingriffsermächtigung aus § 100a StPO darstellt und sich die Auslegung des Telekommunikationsbegriffes in § 100a StPO auch an dem grundrechtlichen Schutz des Betroffenen aus Art. 10 GG orientieren müsse,[428] so ist daraus keinesfalls der nur vermeintlich logische Schluss zu ziehen, dass das BVerfG für eine grundrechtsanaloge Anwendung des Telekommunikationsbegriffes in § 100a StPO streitet. Vielmehr ist dies so zu verstehen, dass die Begriffsauslegung in § 100a StPO nicht weiter gehen darf als der durch Art. 10 GG normierte Schutz des Bürgers. Der Maßstab aus Art. 10 GG deckelt daher die Weite der durch § 100a StPO statuierten Eingriffsbefugnis. Dieses Verständnis wird dadurch gestützt, dass das BVerfG ausführte, dass die vom LG Ellwangen hinsichtlich § 100a StPO vorgenommene Auslegung auch dem Bedeutungsinhalt des eröffneten Art. 10 GG hinreichend gerecht werde und hiermit nicht in Widerspruch stehe[429], da der für rechtmäßig befundene Eingriff auf Grundlage des § 100a StPO sich in den durch Art. 10 GG normierten Grenzen halte. Ein solcher Widerspruch hätte dann bestanden, wenn der Schutzbereich des Art. 10 GG so eng ausgelegt würde, dass das gegenständliche Verhalten nicht hierunter, aber gleichwohl unter die Eingriffsermächtigung des § 100a StPO fallen würde. Aus der Systematik zwischen Grundrechtsschutz und Eingriffsbefugnis und dem Grundsatz des Gesetzesvorbehalts muss daher folgen, dass eine Eingriffsermächtigung nicht zu einem Eingriff ermächtigen darf, dem der Betroffene mangels Einschlägigkeit eines grundrechtlichen Schutzbereichs schutzlos ausgeliefert wäre. Der umgekehrte Schluss, dass die Auslegung im Lichte eines strafprozessualen materiellen Telekommunikationsbegriffes in § 100a StPO nicht restriktiver als in Art. 10 GG erfolgen dürfe bzw. hiermit

426 Vgl. *Durner* in: Maunz/Dürig-GG, Art. 10, Rn. 66; *Nicolai*, HRRS 2021, 365, 368.
427 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 32 = teilweise in NJW 2016, 3508 ff.
428 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 32 = teilweise in NJW 2016, 3508 ff.
429 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13, Rn. 38 = teilweise in NJW 2016, 3508 ff.

im Einklang grundrechtsanalog erfolgen müsse, kann mit Verweis auf die verfassungsgerichtliche Rechtsprechung allerdings nicht geführt werden. Vielmehr entspricht es gängiger Systematik, dass der Schutzbereich im Sinne eines möglichst weiten Grundrechtsschutzes weit zu verstehen ist, während staatliche Eingriffsbefugnisse für einen konkreten Einzelfall gelten und damit eng auszulegen sind.[430] Dass Art. 10 GG als Maßstab für die Auslegung des § 100a StPO ebenfalls herangezogen werden soll, kann daher nur bedeuten, dass der Umfang des Schutzbereichs aus Art. 10 GG den Telekommunikationsbegriff in § 100a StPO in seiner Weite eingrenzt, einer engeren Auslegung als sie in Art. 10 GG stattfindet aber nicht entgegensteht. Im Übrigen führt die Betroffenheit eines Grundrechts lediglich dazu, den diese Betroffenheit auslösenden Eingriff überhaupt an einer Befugnisnorm zu messen, es ist aber allein durch die Betroffenheit eines Grundrechts noch nichts darüber ausgesagt, ob dieser Eingriff auch von der Befugnisnorm gedeckt ist.[431]

cc) Lösung

Es bleibt daher festzuhalten, dass bei zutreffender Zugrundelegung eines strafprozessualen Telekommunikationsbegriffes die passive Informationsgewinnung in Form einer einseitigen Nutzung informationstechnischer Kommunikationsanlagen keine Kommunikation i.S.d. § 100a StPO darstellen kann. Allein aufgrund des Umstandes, dass Informationen bewusst preisgegeben werden, kann noch keine Kommunikation vorliegen. Das bloße Abrufen von Websites oder die Inanspruchnahme der ausgegliederten Rechenleistung des Sprachassistenten zur Informationsbeschaffung kann – selbst, wenn eine mögliche Straffälligkeit dabei evident erscheint (beispielsweise durch den Inhalt der Informationsanfrage: „Wie baue ich eine Bombe?“) keine Telekommunikation im Sinne des § 100a StPO darstellen.[432]

430 ähnlich auch *Wolter/Greco* in: SK-StPO, § 100a StPO, Rn. 13.
431 Zutreffend auch *Kudlich*, JuS 2001, 1165, 1167; *Eckhard*, CR 2001, 385, 387.
432 Zutreffend auch *Trüg/Mansdörfer* in: Hilber, Handbuch Cloud Computing, Teil 7, Rn. 27, die darauf hinweisen, dass Prozesse der Auslagerung von Rechenleistung, Speicher und Arbeitsspeicher oder von Anwendungen wie der Textverarbeitung in der Cloud keine Telekommunikation i.S.d. § 100a StPO darstellen; im Ergebnis auch *Böckenförde*, JZ 2008, 925, 937.

3) Eigener Vorschlag eines strafprozessualen Telekommunikationsbegriffes

Da jedoch nähere Ausführungen zur Ausgestaltung eines genuin strafprozessualen Telekommunikationsbegriffes nur vereinzelt zu finden sind, soll im Folgenden ein weiterer Vorschlag zur Lesart der umstrittenen Voraussetzung des § 100a StPO gemacht werden. Zur Bestimmung eines tauglichen strafprozessualen Telekommunikationsbegriffes ist § 100a StPO im Lichte der gängigen juristischen Auslegungsmethoden zu untersuchen.

a) Erforderliche Personenanzahl

Dabei ist zunächst die Frage zu klären, wie viele Personen an einem Vorgang beteiligt sein müssen, um von Telekommunikation i.S.d. § 100a StPO sprechen zu können.

aa) Auslegung nach Wortsinn

Nach allgemeinem Sprachgebrauch handelt es sich bei Kommunikation um eine Art der Verständigung. Eine tiefergehende Auseinandersetzung anhand des Wortlautes erfordert ebenso einen Blick auf den Wortursprung. Während „Tele“ etwa „in die Ferne“ bedeutet und dabei die räumliche Distanz des Vorgangs beschreibt, fällt unter den Begriff Kommunikation jede Form der Verständigung durch Informationsübermittlung.[433] Kennzeichnend für eine Verständigung ist, dass die jeweiligen Aussagen aufeinander Bezug nehmen. Dabei handelt es sich stets um eine beliebig weite Art der Informationsvermittlung, ohne Einschränkung auf bestimmte Arten der Informationsübermittlung. Aussagen können allerdings nur dann aufeinander Bezug nehmen, wenn diese durch mindestens zwei Personen abgegeben werden. Ansonsten ähnelt der Akt der Kommunikation eher einem Selbstgespräch, jedoch keiner klassischen Kommunikation in Form einer Verständigung.[434]

433 *Gercke*, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren S. 100.

434 So auch *Roxin/Schünemann*, Strafverfahrensrecht, § 36, Rn. 5.

bb) Historische Auslegung

Eine historische Auslegung stellt die Entstehungsgeschichte des Gesetzgebers in den Vordergrund. Unter Zugrundelegung dessen wollte der Gesetzgeber mit der Schaffung des § 100a StPO im Jahr 1968 das Abhören des Fernsprechverkehrs und das Aufzeichnen der dadurch gewonnen Erkenntnisse sicherstellen.[435] Explizit verweist die Gesetzesbegründung darauf, dass den Strafverfolgungsbehörden die Befugnis zum „Telefongespräche abhören"[436] zuteilwerden soll. Es sollte eine Norm geschaffen werden, die es ermöglichte den Informationsaustausch der Täter, den diese infolge des technischen Fortschritts ohne Verlassen der Wohnung und ohne Niederschrift vornehmen konnten, zur Beweisgewinnung verwertbar zu machen.[437] Im Zuge der Neufassung des § 100a StPO durch das Poststrukturgesetz vom 08.06.1989 modifizierte der Gesetzgeber die Befugnis hin zur „Aufzeichnung des Fernmeldeverkehrs". Der Gesetzgeber wollte damit etwaigen Zweifeln an der Anwendbarkeit der Norm hinsichtlich moderner Formen der Nachrichtenübermittlung zuvorkommen.[438] Seit der Entstehung der Norm vermochten Modifizierungen und Anpassung derselben an dem ursprünglich gesetzgeberischen Ziel der Kenntniserlangung von Kommunikationsvorgängen im Ganovenmilieu nichts zu ändern. Für ein solches in der Gesetzesbegründung erwähntes Telefongespräch sind denklogisch zwei Personen erforderlich. Der Gesetzgeber wollte mit der der Schaffung der Norm den Strafverfolgungsbehörden die Möglichkeit geben, sich Kenntnis über ein nicht öffentliches Telefongespräch zwischen zwei Personen verschaffen zu können.

cc) Systematische Auslegung

In systematischer Hinsicht erscheint eine nähere Analyse zunächst schwierig, da der Telekommunikationsbegriff in der StPO im Übrigen nicht zum Vorschein kommt. Möglicherweise kann ein Blick auf § 99 StPO geworfen werden. Dieser erlaubt die Beschlagnahme von Telegrammen und Postsendungen als eine Form der Telekommunikation. Daraus lässt sich jedoch lediglich folgern, dass § 100a StPO nicht für jegliche Art von

435 *Günther* in: MüKo-StPO, § 100a StPO, Rn. 2.
436 BT-Drs, V/1880, S. 6.
437 *Hiéramente/Fenina*, StraFo 2015, 365, 369.
438 BT-Drs. 11/4316, S. 90.

Kommunikation einschlägig ist. Es verdeutlicht daher die Notwendigkeit eines strafprozessual anhand von § 100a StPO gebildeten Telekommunikationsbegriffes, liefert aber für dessen genauere Ausgestaltung keine zielführenden Anhaltspunkte. Zielführend erscheint ein Vergleich auf welche Art und Weise die Daten durch die §§ 100a ff. StPO gewonnen werden sollen. Während die Datengewinnung bei § 100a StPO durch den Zugriff auf einen Kommunikationsvorgang im Ganovenmilieu erfolgt, soll dies bei § 100b StPO vielmehr durch Infiltration eines informationstechnischen Systems erfolgen. Bei § 100c StPO wiederum erfolgt die Informationsgewinnung durch das Verwanzen der Wohnung des Betroffenen. Nach einem Vergleich dieser Normen wird daher ersichtlich, dass im Rahmen des § 100a StPO im Unterschied zu § 100b und c StPO mehrere Personen in den Vorgang auf welchen zugegriffen wird involviert sein müssen. § 100b StPO und 100c StPO erlauben hingegen auch den Zugriff auf einen unipersonal stattfindenden Vorgang in Form der Überwachung der Kommunikation einer Person mit ihren eigenen Daten[439] oder dem Abhören eines Selbstgesprächs im Rahmen des § 100c StPO.[440]

dd) Teleologische Auslegung

Schließlich ist die Norm auch nach ihrem Telos zu untersuchen. Dieser liegt darin, die Aufklärung von Straftaten durch heimliche Beweisgewinnung zu ermöglichen.[441] Diesem Zweck dienen jedoch letztlich sämtliche Normen der § 100a ff. StPO. Daher ist weiter zu beleuchten, welche Art von Erkenntnissen § 100a StPO im Unterschied zu anderen Ermittlungsbefugnissen hervorbringen soll. Hierzu wurde eine Unterscheidung zwischen Daten und Informationen vorgeschlagen.[442] Allerdings haben die § 100a ff. StPO im Ergebnis allesamt die Erlangung von Informationen und nicht lediglich bloßer Daten zum Ziel. Zielführender erscheint es daher im Zuge der Auslegung zu ermitteln, welche Erkenntnisse durch eine ausgewählte Zwangsmaßnahme hervorgebracht werden sollen. Die erhofften Erkenntnisse zielen auf getroffene Absprachen und Mitteilungen

439 *Sinn*, Stellungnahme zum Entwurf der BT-Drs. 18/11272, S. 5.
440 Vgl. BGHSt 50, 206. Neben dem möglichen Zugriff auf ein solches Selbstgespräch über § 100c StPO ist hinsichtlich dessen anschließender Verwertbarkeit anhand der Maßstäbe des Kernbereichsschutzes zu entscheiden.
441 *Gercke* Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, S. 106.
442 *Demko*, NstZ 2004, 57, 61 mit Verweis auf *Weßlau*, ZStW 2001, 681, 689.

zur Planung, Durchführung oder (Nach-) Besprechung einer Straftat. Solche Absprachen können jedoch nur durch mehrere Personen erfolgen, da der schlichte Einzeltäter in der Regel mangels Mittäter oder Beteiligter mit niemanden über die Tat sprechen wird. Tut er dies doch, so würde er, selbst wenn er die Tat allein auszuführen gedenkt, deren Begehung wiederum mit einer anderen Person besprechen. Hierdurch läge wiederum eine Verständigung über die Planung der Tat und damit Kommunikation vor. Da gerade solche Erkenntnisse der Planung oder auch (Nach-)Besprechung einer Tat gewonnen werden sollen, kommt man ebenfalls zum Schluss, dass solche Erkenntnisse nur dann generiert werden können, wenn mehrere Personen an einem Telekommunikationsvorgang beteiligt sind.

Mit Blick auf das Bild, welches der Gesetzgeber bei der Schaffung der Norm vor Augen hatte (Telefongespräche abhören), muss zudem gefordert werden, dass der Vorgang der Telekommunikation dazu dienen muss, einer menschlichen Person eine Nachricht zu übermitteln.[443] Ganz außer Acht bleiben soll auch in diesem Zusammenhang die vielfach zitierte „Entwicklungsoffenheit des § 100a StPO“[444] nicht. Dabei ist jedoch strikt zwischen der Entwicklungsoffenheit auf Ebene des Art. 10 GG und des § 100a StPO zu trennen. Auf Ebene des § 100a StPO bedeutet diese Entwicklungsoffenheit, dass neben dem klassischen Telefongespräch auch Kommunikation mittels SMS, E-Mails, Chatnachrichten oder Internettelefonie überwacht werden darf.[445] Allerdings ändert auch ein solcher Wechsel des Kommunikationsmediums nichts daran, dass stets Telekommunikation im Sinne einer Nachrichtenübermittlung an eine andere Person im Zusammenhang mit etwaiger Ganovenkommunikation, wie es der Gesetzgeber bei der Kodifizierung des § 100a StPO vorgesehen hatte, im Vordergrund stehen muss. Offenbaren sich im Zuge der technischen Entwicklung wesensverschiedene Anwendungsmöglichkeiten zu dem angedachten Anwendungsfall, bei denen eben nicht mehr die klassische Ganovenkommunikation im Vordergrund steht, so können diese nicht von dem strafprozessualen Telekommunikationsbegriff aus § 100a StPO umfasst sein. Eine solche Ganovenkommunikation kann jedoch denklogisch nur zwi-

443 Ähnlich auch *Meinicke*, DSRITB 2013, 967, 971, wonach § 100a StPO originär für die Überwachung der Kommunikation zwischen zwei Individuen konzipiert sei.

444 *Bruns* in: KK-StPO, § 100a StPO, Rn. 4; *Hiéramente/Fenina*, StraFo 2015, 365, 370, m.w.N.

445 Zutreffend in diese Richtung auch *Hiéramente/Fenina*, StraFo 2015, 365, 370.

schen Mittätern oder Täter und Gehilfe von Statten gehen. Auch im Lichte einer teleologischen sind für Telekommunikation i.S.d. § 100a StPO daher zwei Menschen erforderlich.[446]

b) Telekommunikationswille

In der Vergangenheit ist es immer wieder vorgekommen, dass zum einen während des Abhörvorgangs beispielsweise auch auf Hintergrundgespräche, die eigentlich nicht Teil der unmittelbar überwachten Kommunikation darstellten und auf den ersten Blick daher eher unter § 100c StPO fallen mögen, zugegriffen wurde oder zum anderen mitgehört wurde, nachdem eine Verbindung nur versehentlich hergestellt oder nicht vollständig beendet wurde.[447] Ob solche Gespräche jedoch unter den Telekommunikationsbegriff fallen, entscheidend sich letztlich danach, ob für das Vorliegen von Telekommunikation ein Telekommunikationswille erforderlich ist.

Der Wortlaut des § 100a StPO enthält keine unmittelbaren Anhaltspunkte hinsichtlich der subjektiven Sichtweise des Betroffenen. Die Frage, ob man sich nur verständigen könne, wenn hierfür ein entsprechender Wille vorhanden ist, ließe sich mit dem Argument verneinen, dass Menschen vielfach kommunizieren, ohne sich hierüber bewusst zu sein, etwa durch Mimik oder Gestik. Die gesamte non-verbale Kommunikation über Körperhaltung und Ausdruck läuft daher beinahe täglich ohne ausdrücklichen Kommunikationswillen ab. Dabei ist allerdings zu beachten, dass es sich im Rahmen des § 100a StPO lediglich um verbale Kommunikation handelt. Eine solche ist unter normalen Umständen nicht ohne den Willen zur Kommunikation möglich. Selbst bei einem Selbstgespräch – das im Regelfall aufgrund des fehlenden Kommunikationspartners – nicht unter § 100a StPO fällt, handelt der Sprechende in dem Bewusstsein nun eben mit sich selbst zu kommunizieren. Ausgehend vom Wortsinn der Kommunikation müsste man daher das Vorliegen eines Kommunikationswillens als erforderlich erachten. Systematische und historische Auslegung helfen an dieser Stelle ebenfalls nicht weiter. Vergegenwärtigt man sich erneut Sinn und Zweck einer heimlichen Aufklärung von Straftaten könnte man auf einen Telekommunikationswillen verzichten. Schließlich soll Ziel einzig und allein das Erlangen belastbarer Informationen durch den Zugriff auf Telekommunikationsmedien sein.

446 So auch *Eidam*, NJW 2016, 3511, 3512.
447 Vgl. BGH, NJW 2003, 2034, 2035.

Auch die Rechtsprechung hatte sich in der Vergangenheit häufiger mit der Frage nach dem Vorliegen eines Kommunikationswillen sowie mit den möglichen Anforderungen an diesen zu beschäftigen. Das BVerfG urteilte, dass der Betroffene zumindest über ein potenzielles Bewusstsein verfügen müsse, in jenem Moment nach außen zu kommunizieren.[448] Auch der BGH urteilte zur Verwertbarkeit eines sog. Raumgesprächs in die gleiche Richtung. Während der Zugriff auf ein Raumgespräch eigentlich den klassischen Anwendungsfall des § 100c StPO wiedergibt, soll unter gewissen Voraussetzungen, auf das während eines solchen Raumgesprächs Gesprochene auch über § 100a StPO zugegriffen werden können. Voraussetzung hierfür ist gerade nicht, dass sich der konkrete Vorgang mit aktuellem Willen oder Wissen der betroffenen Person vollzieht.[449] Nach den Ausführungen der Richter am Bundesgerichtshof ist jedoch erforderlich, dass *„nach willentlicher Herstellung einer Telekommunikationsverbindung durch die Zielperson […] aus deren Sicht versehentlich [Informationen] übertragen werden"*[450]. Entscheidend soll also sein, dass der Betroffene die Verbindung selbst hergestellt oder die versehentliche Aufrechterhaltung durch ihn verursacht wurde. Dabei genügt es bereits, wenn der Betroffene das Telekommunikationsmedium in Betrieb setzt oder in betriebsbereitem Zustand hält.[451] Dem folgend würde dann wohl bereits in einem Fall, in dem der Betroffene sein Mobiltelefon ohne Tastatursperren in der Tasche trägt und durch die Gehbewegung unbemerkt und ungewollt eine Verbindung hergestellt wird, die notwendigen Voraussetzungen für einen Telekommunikationswillen erreicht sein.[452]

Es wird deutlich, dass die Anforderungen an einen vorhandenen Telekommunikationswillen äußerst gering sind. Diese geringen Anforderungen zugrunde liegend erscheint es bereits überaus fraglich überhaupt noch von einem wirklichen Willen zur Telekommunikation zu sprechen. Vielmehr entsprechen die entwickelten Maßstäbe eher einer Einordnung in Risikosphären. So wie das Telekommunikationsmedium in Betrieb genommen wurde, ist es der Nutzer, der für sämtliche „Selbstständigkeiten" seines Gerätes verantwortlich ist. Er trägt das Risiko, dass auf eine sodann auch ohne sein Wissen aufgebaute oder nicht beendete Verbindung von

448 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 20 = teilweise in NJW 2016, 3508 ff.
449 BGH, NJW 2003, 2034, 2035.
450 BGH, NJW 2003, 2034, 2035.
451 BGH, NJW 2003, 2034, 2035.
452 *Gercke*, JZ 2004, 347, 348.

Seiten des Staates zugegriffen werden kann. Das Kriterium der Veranlassung stellt einen sachgerechten Mittelweg zwischen dem Erfordernis eines vollständig notwendigen Kommunikationswillens und dem kompletten Verzicht hierauf dar. Das Erfordernis eines Telekommunikationswillen, dem sich der Betroffene vollumfänglich bewusst ist, würde zu erheblichen Beweisschwierigkeiten führen. Die Strafverfolgungsbehörden müssten den entsprechenden Willen prozessrechtlich nachweisen, was vielfach nicht gelingen würde. Auf der anderen Seite würde ein gänzlicher Verzicht auf ein solches Kriterium die Freiheit des Einzelnen zu sehr einengen und die Ermächtigungsgrundlage des § 100a StPO zu sehr in die Nähe des § 100c StPO rücken lassen. Sofern dem Nutzer eine willensgesteuerte Veranlassung zugeschrieben werden kann, wurde das Abhören der Gespräche nicht gezielt durch die Strafverfolgungsbehörden forciert, sondern erst durch möglicherweise fahrlässiges Handeln der Betroffenen, die den ursprünglichen Telekommunikationsvorgang in Gang setzen, ermöglicht. Diese haben den Vorgang durch Ihr Handeln veranlasst und damit den Strafverfolgungsbehörden erst die Möglichkeit gegeben Erkenntnisse zu sammeln.[453] Daher ist zu konstatieren, dass sofern die übrigen Voraussetzungen für Telekommunikation vorliegen, es sich bereits dann um Telekommunikation i.S.d. § 100a StPO handeln kann, wenn diese jedenfalls menschlich veranlasst oder in Gang gesetzt wurde.

c) Zwischenergebnis

Unter Berücksichtigung dessen ist Kommunikation i.S.d. § 100a StPO jeder menschlich veranlasste Vorgang, der nach seinem objektiven Verständnis unmittelbar dazu dient oder dienen sollte, eine Mitteilung an eine nicht mit dem Veranlasser des Vorgangs identische menschliche Person zu übermitteln. Dass die Nachricht an einen menschlichen Empfänger gerichtet werden muss, stellt sicher, dass die Antwort des Empfängers individuell und nicht aufgrund einer mathematischen oder technischen Formel zu Stande gekommen ist. Solch eine „berechnete" Antwort wäre mit dem Verständnis der Kommunikation in § 100a StPO nicht vereinbar, da ein für Kommunikation immanentes Erfordernis fehlen würde. Die zu erwartende Antwort darf gerade nicht technisch und objektiv vorhersehbar sein. Damit aus Kommunikation schließlich Telekommunikation im Sinne des § 100a StPO wird muss der beschriebene Vorgang der Mitteilungsüber-

453 A.A. *Fezer*, NstZ 2003, 625, 628.

mittlung durch ein technisches Mittel geschehen, das nach seinem objektivem Verständnis für die Nachrichtenübermittlung in die Ferne geschaffen wurde.[454] Zusammenfassend ist der Begriff der Telekommunikation im Rahmen des § 100a StPO nicht synonym zum Telekommunikationsbegriff des Art. 10 GG auszulegen, sondern es ist vielmehr ein eigener personell-individueller Telekommunikationsbegriff heranzuziehen.

d) Nutzung eines Sprachassistenten in der Form eines Smart Speakers im Sinne des personell-individuellen Telekommunikationsbegriffs

Es bleibt zu klären, inwiefern bei der Nutzung eines Smart Speakers unter Zugrundelegung des personell-individuellen Telekommunikationsbegriffs von Telekommunikation gesprochen werden kann. Sofern direkt auf die Hardware des Smart Speakers zugegriffen werden soll und hierauf gespeicherte Informationen erlangt werden sollen, fehlt es an einem erforderlichen Übermittlungsvorgang. Es würde keine Telekommunikation vorliegen. Da sich der personell-individuelle Telekommunikationsbegriff nicht an der Legaldefinition des § 3 Nr. 22 TKG orientiert, wäre es für ein Übersenden bereits ausreichend, wenn dieses zwar noch nicht stattfand, jedoch im nächsten Moment ohne weiteres zutun des Nutzers erfolgen würde. Auch im Stadium der Übermittlung der Audiodatei zum Sprachassistenten liegt nach diesem Begriffsverständnis aber aus mehreren Gründen keine Telekommunikation vor. Zum einen fehlt es bereits an dem Erfordernis zweier menschlicher Personen. Hinzu kommt, dass die Antwort des Sprachassistenten aufgrund bestimmter Algorithmen berechnet wurde, ihr mithin die notwendige Individualität abhandenkommt. Daher fehlt es an der erforderlichen Verständigung in Form einer individuell aufeinander eingehenden Konversation. Zum anderen ist zu beachten, dass ein Sprachassistent grundsätzlich ein Mittel zur Informationsgewinnung, nicht jedoch zur Informationsübertragung darstellt. Dieser Funktion ist sich auch der Nutzer eines Sprachassistenten bewusst. Würde auf diesen dennoch unter Heranziehung des § 100a StPO zugegriffen, so würde dessen eigentliche Funktion umfunktioniert. Für Zugriffe auf solche Arten

454 Tele entstammt dem griechischen tēle und wird im deutschen Sprachgebrauch mit fern/weit assoziiert, vgl. https://de.wiktionary.org/wiki/tele-#:~:text=%5B1%5D%20vorangestelltes%20Wortbildungselement%20in%20Fremdw%C3%B6rtern,tele)%20%E2%86%92%20grc%20%E2%80%9Efern%E2%80%9C (zuletzt abgerufen am 31.10.2021).

von digitalen technischen Geräten ist § 100a StPO nach dessen Sinn und Zweck nicht geschaffen. Bei dem Zugriff auf einen Sprachassistenten steht gerade nicht die Verständigung zwischen zwei Personen aus dem Ganovenmilieu im Vordergrund, sondern eine Kenntniserlangung hinsichtlich der durch den Betroffenen durchgeführten Informationsabfragen. Auch sofern sich die Daten bereits auf den Servern des Dienstleisters befinden, ergibt sich kein anderes Bild. Es fehlt an den grundlegenden Voraussetzungen, um von Telekommunikation im Sinne des § 100a StPO sprechen zu können. Somit bleibt festzuhalten, dass § 100a StPO keine taugliche Ermächtigungsgrundlage zum Zugriff auf die durch Sprachassistenten erlangte Informationen bietet.

4) Verschlüsselung der Daten

Ein weiteres Problem, dem sich ein Zugriff nach § 100a Abs. 1 S. 1 StPO gegenübersieht, liegt darin begründet, dass die Daten während des Übertragungsweges von Hardware zum Server verschlüsselt übertragen werden.[455] Um diesem technischen Fortschritt Rechnung zu tragen, wurden die Vorschriften in Form von § 100a Abs. 1 S. 2, 3 StPO geschaffen.[456] Neben der Frage, inwiefern unter Zuhilfenahme dieser neugeschaffenen Normen auf Sprachassistenten zugegriffen werden könnte, sehen sich diese Normen auch verfassungsrechtlichen Bedenken gegenüber. Auf jene Problemfelder soll im Folgenden näher eingegangen werden.

II) § 100a Abs. 1 S. 2 StPO n.F.

1) Allgemeines

Bezüglich unverschlüsselter Daten hat der Dienstleistungsanbieter nach §§ 100a Abs. 4 StPO, 110 Abs. 1 TKG die erforderlichen technischen Vorkehrungen zu treffen, um den Behörden eine Kopie der zu überwachenden Telekommunikationsinhalte zur Verfügung stellen können, sodass die Erlangung solcher Daten – die Einschlägigkeit des § 100a StPO vorausge-

455 vgl. https://support.apple.com/de-de/HT202303 (zuletzt abgerufen am 31.10.2021).

456 BT-Drs. 18/12785, S. 48; *Bruns* in: KK-StPO, § 100a StPO, Rn. 42.

setzt – keine größeren Probleme bereiten würde.[457] Nachdem jedoch inzwischen ein Großteil der über das Internet laufende Kommunikation verschlüsselt erfolgt[458], werden den Ermittlungsbehörden nach erfolgter Aufzeichnung durch den Dienstleistungsanbieter oft nur verschlüsselte Daten geliefert. Die Daten werden lediglich in kryptierter Form aufgezeichnet, ohne dass dem Dienstleistungsanbieter oder den Strafverfolgungsbehörden ein Zugriff auf die unverschlüsselten Kommunikationsinhalte möglich ist. Deren Entschlüsselung wiederum würde die Behörden vor technisch nicht zu überwindende Hürden stellen oder sich jedenfalls langwierig und kostenintensiv gestalten.[459] Ganz im Gegenteil ist es sogar ein gesetzgeberisches Anliegen zum Schutze vertraulicher Daten vor Zugriffen Dritter eine Weiterentwicklung und Verbesserung der Verschlüsselungstechnologien herbeizuführen.[460] Die Stärkung des Datenschutzes ohne eine gleichzeitige gesetzgeberische Reaktion hinsichtlich der staatlichen Ermittlungsbefugnisse, würde jedoch die Ermächtigung des § 100a Abs. 1 S. 1 StPO zu einem stumpfen Schwert verkommen lassen. Um auch weiterhin eine effektive Strafverfolgung zu gewährleisten, muss somit eine Überwachung direkt an der Quelle, und noch vor erfolgter Verschlüsselung möglich sein. Bei der Nutzung eines Sprachassistenten würden dann durch das Mikrofon aufgezeichnete Audiosignale noch vor der verschlüsselten Übermittlung an den Server abgegriffen.

2) Verfassungsmäßigkeit des § 100a Abs. 1 S. 2 StPO n.F.

Zur technischen Umsetzung dieses Vorhabens ist die Installation einer Software zur Ausleitung der Kommunikation vor deren Verschlüsselung notwendig.[461] Hierfür eröffnen sich den Ermittlungsbehörden grundsätz-

457 *Bruns* in: KK-StPO, § 100a StPO, Rn. 37.

458 „*Viele Apple-Dienste verwenden eine Ende-zu-Ende-Verschlüsselung, was bedeutet, dass nur du auf deine Daten zugreifen kannst, und zwar nur auf vertrauenswürdigen Geräten, auf denen du mit deiner Apple-ID angemeldet bist.In einigen Fällen können deine iCloud-Daten auf den Servern von Drittanbietern – wie Amazon Web Services oder Google Cloud Platform – gespeichert werden, aber diese Partner haben nicht die Schlüssel, um deine auf ihren Servern gespeicherten Daten zu entschlüsseln*“, vgl. https://support.apple.com/de-de/HT202303 (zuletzt abgerufen am 31.10.2021).

459 BT-Drs. 18/12785, S. 48.

460 BT-Drs. 18/12785, S. 48.

461 *Bruns* in: KK-StPO, § 100a StPO, Rn. 42; *Bär* in: BeckOK-PolR Bayern, Art. 42 PAG, Rn. 93.

lich zwei verschiedene Wege. Da § 100a Abs. 1 StPO keine Erlaubnis zum Betreten einer Wohnung beinhält, bleibt letztlich nur die Infiltration des Systems über das Internet. Hierüber kann zum einen unter Ausnutzung bestehender Sicherheitslücken des Systems ein Trojanisches Pferd aufgespielt werden.[462] Andernfalls ist eine Infiltrationsmethode zu wählen, die eine aktive Aktion des Betroffenen erfordern. Beispielweise kann mittels eines per E-Mail verschickten Anhangs, welcher den Empfänger zum Öffnen animiert, der Trojaner installiert werden.[463]

Hinsichtlich des grundrechtlichen Schutzes der Betroffen solcher infiltrierter technischer Systeme hob das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung aus dem Jahr 2008 hervor, dass das allgemeine Persönlichkeitsrecht auch ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) enthält.[464] Dies war erforderlich, da das Gericht den bisherigen Grundrechtsschutz zum Schutz informationstechnische Systeme, „*die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten*“[465] nicht für genügend erachtete. Art. 13 GG biete weder Schutz vor Zugriffen gegen die Infiltration eines informationstechnischen Systems noch vor einer Datenerhebung aus den Datenspeichern, selbst wenn sich dieses System in der eigenen Wohnung befinde.[466] Anders als das Grundrecht auf informationelle Selbstbestimmung, das vor der einzelnen Datenerhebung als solcher schützt[467], soll das IT-Grundrecht den Einzelnen vor einem Zugriff auf die Gesamtheit der in informationstechnischen Systemen umfangreich vorhandenen persönlichen Daten bewahren.[468] Auch das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf informationelle Selbstbestimmung, das zwar Gefährdungen für die Persönlichkeitsentfaltung verhindern soll, kann im Falle der Infiltration eines informationstechnischen Systems diesen Schutz möglicherweise nicht immer bieten. Beim Zugriff auf ein komplettes System stehen dem Zugreifenden äußerst große und aussagekräftige Datenbe-

462 *Popp*, ZD 2012, 51, 52; *Skistims/Roßnagel*, ZD 2012, 3, 3 f.
463 *Hansen/Pfitzmann*, DRiZ 2007, 225, 227.
464 BVerfGE 120, 274 ff.
465 BVerfGE 120, 274, 314.
466 BVerfGE 120, 274, 310.
467 *Gersdorf* in: BeckOK-InfoMedienR, Art. 2 GG, Rn. 17 f.
468 BVerfGE 120, 274, 313.

stände zur Verfügung. Das Gewicht eines solchen Zugriffs für die eigene Persönlichkeit gehe weit über das einzelner Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, hinaus.[469] Ein solcher Eingriff in die Integrität eines informationstechnischen Systems, stellt daher im Gegensatz zur klassischen Telefonüberwachung beim Telekommunikationsanbieter ein qualitatives Mehr dar, weshalb ein solcher Eingriff naturgemäß schwerer wiege.[470][471] Mit der Infiltration eines informationstechnischen Systems zum Zweck der Quellentelekommunikationsüberwachung sei bereits der Grundstein gelegt, um das System insgesamt zu durchleuchten. Hierdurch komme es zu einer Gefährdungssituation, die weit über die hinausgehe, die mit einer bloßen Überwachung der laufenden Telekommunikation einhergehen würde.[472] Den damit einhergehenden spezifischen Gefährdungen der Persönlichkeit des Einzelnen mitsamt der Möglichkeit der Strafverfolgungsbehörden ein komplettes Persönlichkeitsprofil zu erstellen, könne das Fernmeldegeheimnis allein nicht oder nicht hinreichend begegnen.[473] Ein tatsächlicher Eingriff in ein informationstechnisches System im Sinne einer Eröffnung des Schutzbereichs des IT-Grundrechts ist jedoch nur dann anzunehmen, wenn durch die Infiltration des Systems eine Datenfülle gewonnen werden könnte, die einen tiefen Einblick in die persönlichen Lebensverhältnisse des Einzelnen gewährt.[474] Hiervon ist nur dann auszugehen, wenn das Zielsystem komplett durchleuchtet werden soll und auch bereits gespeicherte Daten gescannt werden. Sofern die Ermittlungsbehörden lediglich auf „laufende", aber aufgrund fortschreitender Technik verschlüsselte Kommunikation zugreifen, darf das informationstechnische System daher derart infiltriert werden, dass zwar eine Ausleitung laufender Kommunikation möglich ist,

469 BVerfGE 120, 274, 313.
470 *Stadler*, MMR 2012, 18, 19; *Popp*, ZD 2012, 51, 53.
471 Aufgrund dieses Umstands und weil die §§ 100a, b StPO a.F. keine Einschränkung dahingehend enthielten, dass lediglich laufende Telekommunikation aufgezeichnet werden dürfe, konnten diese Normen vor Schaffung des § 100a Abs. 1 S. 2 StPO aufgrund eines Verstoßes gegen den Wesentlichkeitsvorbehalt, der den Gesetzgeber verpflichtet, für eingriffsintensive Maßnahme eine gesetzliche Grundlage zu schaffen, keinesfalls als Befugnisnorm für eine Quellentelekommunikationsüberwachung herangezogen werden. Somit war es nur folgerichtig, dass mit § 100a Abs. 1 S. 2 StPO hierzu eine neue Befugnis geschaffen wurde. A.A. LG Landshut, Beschluss vom 20.1.2011 – 4 Qs 346/10; *Bär*, MMR 2011, 691, 692 f.
472 BVerfGE 120, 274, 308.
473 BVerfGE 120, 274, 309.
474 BVerfGE 120, 274, 313 ff.

jedoch nicht auf gespeicherte Inhalte zugegriffen und diese durchleuchtet werden können. Sodann liegt kein Eingriff in das IT-Grundrecht vor, sondern lediglich ein solcher in das Telekommunikationsgeheimnis des Art. 10 GG.[475] Das Telekommunikationsgeheimnis sieht sich in einem solchen Fall lediglich den Gefährdungen gegenüber, für die das Grundrecht ursprünglich geschaffen wurde: Den Schutz laufender Telekommunikation.

Problematisch bleibt, dass die Eingriffsintensität der Quellen-TKÜ über die des herkömmlichen Anwendungsfalls des § 100a Abs. 1 S. 1 StPO hinausgeht. Es kommt zu einem Zugriff auf die Telekommunikation bereits auf dem Gerät des Betroffenen, also schon unmittelbar vor einem eigentlich erforderlichen dynamischen Übermittlungsvorgang. Dies lässt leichte Parallelen zur Online-Durchsuchung erkennen. Der entscheidende Unterschied zu einer Parallelität mit der Online-Durchsuchung liegt allerdings darin, dass auch § 100a Abs. 1 S. 2 StPO lediglich den Zugriff auf „laufende" Kommunikation erlaubt. Die Infiltration des Systems darf technisch lediglich zulassen, die zum aktuellen Zeitpunkt ausgehende Kommunikation vor deren Verschlüsselung auszuleiten. Hingegen darf nicht auch auf gespeicherte Daten oder sonstige auf dem System gespeicherte Kommunikation zugegriffen werden.[476] Auch nach der Implementierung solcher gesetzlichen Schranken, die verbieten auf ruhende Kommunikation zuzugreifen, bestehen Bedenken, dass diese nicht garantieren können, dass tatsächlich lediglich auf „laufende" Telekommunikation zugegriffen wird.[477] Hierzu hat das BVerfG hinsichtlich dem präventiv angelegten Pendant zur Quellentelekommunikation in Form des § 20l Abs. 2 BKAG a.F. entschieden, dass „*ob oder wie sich durch technische Maßnahmen sicherstellen lässt, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird, […] die Anwendung der Norm, nicht aber ihre Gültigkeit [betrifft].*

475 BVerfGE 141, 220, Rn. 228; *Buermeyer*, StV 2013, 470, 473.

476 BT-Drs. 17/12541, S. 78; hinsichtlich der technischen Möglichkeit dieser Begrenzung siehe *Fox,* Stellungnahme, S. 8. Danach kann der Leistungsumfang einer installierten Durchsuchungssoftware erheblich variieren und auf verschiedene Funktionen, wie beispielsweise auf das Abfangen von gesendeten und empfangenen elektronischen Nachrichten, mithin dem Anwendungsfall der Quellentelekommunikation, begrenzt und ausgeweitet werden.

477 Diese technischen Zweifel beziehen sich darauf, dass bei der Scannung eines Systems keine Selektion zwischen gespeicherten Daten und gespeicherten übertragenen Daten, die sodann einer ehemals laufenden Telekommunikation zuzuordnen wären, möglich ist, da die auf dem Rechner bereits gespeicherten Daten keine eindeutigen und verlässlichen Kennzeichnungen verschiedener Dateninhalte enthalten, vgl. *Freiling*, Stellungnahme, S. 6.

[…] Das Gesetz lässt jedenfalls keinen Zweifel, dass eine Quellen-Telekommunikationsüberwachung nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation erlaubt ist".[478] Allein der Umstand, dass infolge eines Missbrauchs oder ähnlichem bei der durchgeführten Infiltration die Gefahr eines vollständigen Durchleuchtens besteht, stellt daher eine bloße Frage der Gesetzesanwendung dar und lässt die Gültigkeit der Norm unberührt. Diesen Anforderungen kommt § 100a Abs. 5 Nr. 1a StPO nach, der inhaltsgleich zum alten § 20l Abs. 2 BKAG a.F. formuliert ist.

Die Schaffung des § 100a Abs. 1 S. 2 StPO entbindet jedoch nicht von einer exakten Prüfung, ob es sich bei dem Verhalten, auf welches zugegriffen werden soll, um Telekommunikation im Sinne des § 100a StPO handelt. Denn die Gesetzesänderung diente ausschließlich dazu, mit den technischen Entwicklungen der Informationstechnik Schritt zu halten und – ohne auf gespeicherte Daten des informationstechnischen Systems zuzugreifen – eine Telekommunikationsüberwachung auch dort durchführen zu können, wo diese auf Basis der alten Überwachungstechnik ansonsten nicht mehr realisierbar gewesen wäre.[479] Insofern kann auf die verschiedenen Interpretationsmöglichkeiten zum Telekommunikationsbegriff verwiesen werden. Mithin liegt bei einer vorzuziehenden strafprozessualen Ausgestaltung des Telekommunikationsbegriffes auch hier keine Telekommunikation vor. Fraglich ist jedoch, zu welchem Ergebnis in dieser Fallgestaltung, die vor allen Dingen von der Rechtsprechung favorisierte technikorientiere Auffassung gelangen würde. Schließlich erfolgt der eigentliche Zugriff vor der Verschlüsselung und damit vor dem Aussenden dieser Daten.[480] Bei strikter Zugrundelegung der Legaldefinition aus § 3 Nr. 22 TKG erscheint es daher zunächst schwierig, im Zugriff vor der verschlüsselten Übertragung bereits ein Aussenden, Übermitteln oder Empfangen von Signalen zu erblicken. Vielmehr ähnelt der Zugriff im Rahmen der Quellen-Telekommunikationsüberwachung einem Zugriff im zeitlichen Stadium, zu dem sich die Daten noch auf dem Gerät vor Ort befinden. Für einen Zugriff vor der Übertragung wurde allerdings bereits dargelegt, dass mangels eines dynamischen Übermittlungsvorgangs ein Zugriff direkt auf das Gehäuse sowohl nach der rein technischen als auch nach der technikorientierten Auffassung ausscheiden müsse. Allerdings würde eine solche restriktive Auslegung den Sinn und Zweck des neu

478 BVerfGE 141, 220, Rn. 234.
479 GesBegr. BT-Drs. 18/12785, S. 50.
480 *Becker/Meinicke*, StV 2011, 50, 51.

geschaffenen § 100a Abs. 1 S. 2 StPO vereiteln. Ziel der Quellen-TKÜ ist schließlich gerade die Überwachung von Telekommunikation direkt an der Quelle, noch bevor diese vor der Übertragung verschlüsselt werden kann.[481] Die Rechtsprechung hat sich seit Einführung des § 100a Abs. 1 S. 2 StPO hierzu noch nicht geäußert, es ist jedoch anzunehmen, dass sie dieses dogmatische „Problemchen" unter Berufung auf Sinn und Zweck der Gesetzesänderung löst. Gleichwohl würde sich bei Zugrundelegung des vorzuziehenden personell-individuellen Telekommunikationsbegriffes diese Frage freilich schon gar nicht stellen. Da der Zugriff unmittelbar vor Verschlüsselung der Daten erfolgt und diese sich im nächsten Moment im Übermittlungsvorgang befinden, würde dieser Umstand das Vorliegen von Telekommunikation nicht hindern. Im Gesamten entspricht § 100a Abs. 1 S. 2 StPO daher den verfassungsrechtlichen Vorgaben.

3) Informationstechnisches System

a) Allgemeines

Obwohl sich das Bundesverfassungsgericht in der Entscheidung zur Online-Durchsuchung ausgiebig zum IT-Grundrecht äußerte, hielt sich das Gericht mit Ausführungen zum Begriff des informationstechnischen Systems zurück. Überblicksartig wurde darauf verwiesen, dass die Informationstechnik einen beträchtlichen Teil im Leben der Bevölkerung einnehme und sich in einer Vielzahl der Gegenstände befinden, die die Bürger täglich umgeben.[482] Diese oberflächliche Beschreibung ist dahingehend zu präzisieren, dass ein informationstechnisches System selbst im Rahmen des Datenverarbeitungsprozesses neben den gespeicherten Daten des Nutzers weitere Daten erzeugen muss, die gleichfalls hinsichtlich seines Verhaltens ausgewertet werden können.[483] In der Literatur wird die Rechtsprechung des Bundesverfassungsgericht teilweise derart verstanden, dass nur solche Systeme, die einen äußerst großen und aussagekräftigen Datenbestand aufweisen und somit Rückschlüsse auf wesentliche Teile der Lebensgestaltung ermöglichen, als informationstechnische Systeme zu verstehen seien.[484] Dieser Schluss geht jedoch fehl. Das Bundesverfassungsgericht

481 BT-Drs. 17/12541, S. 78.
482 BVerfGE 120, 274, 304.
483 *Hauck* in: LR-StPO, § 100a StPO, Rn. 101.
484 *Hauck* in: LR-StPO, § 100a StPO, Rn. 102.

hat diese Formel lediglich zur Abgrenzung des allgemeinen Persönlichkeitsrechts in Form des Rechts auf informationelle Selbstgestaltung und des IT-Grundrechts verwendet. Ein informationstechnisches System kann jedoch sowohl in dem einen als auch in dem anderen Fall vorliegen und betroffen sein. Im von der „Gegenauffassung" zitierten Urteil formuliert das BVerfG an der entsprechenden Stelle sogar ausdrücklich, dass „*nicht jedes informationstechnische System […] des besonderen Schutzes durch eine eigenständliche pesönlichkeitsrechtliche Gewährleistung [bedarf]*".[485] Dadurch wird deutlich, dass auch ein informationstechnisches System betroffen sein kann, ohne dass der Schutzbereich des IT-Grundrechts eröffnet ist. Eine Infiltration eines informationstechnischen Systems wird erst dann einen Eingriff in das strengeren Rechtfertigungsanforderungen unterworfene IT-Grundrecht darstellen[486], wenn dadurch eine Vielzahl persönlichkeitsrelevanter Daten über die eigene Lebensgestaltung gewonnen würden. Dies wird regelmäßig erst bei einem Zugriff auf eine komplette, auf einem informationstechnischen System ruhende Datensammlung der Fall sein.

b) Doppelnatur

Auch der Begriff des informationstechnischen Systems offenbart – ähnlich zum Begriff der Telekommunikation aus § 100a StPO – eine Doppelnatur. Auf der einen Seite stellt das informationstechnische System das Schutzgut des IT-Grundrechts dar, was aus einer verfassungsrechtlichen Perspektive betrachtet wiederum ein weites Begriffsverständnis für angezeigt erscheinen lässt. Auf der anderen Seite handelt es sich um das Zugriffsobjekt einer strafprozessualen Ermittlungsmethode, was wiederum ein eher enges Verständnis erforderlich macht.[487]

485 BVerfGE 120, 274, 313.

486 Vgl. *Hoffmann-Riem*, JZ 2008, 1009, 1015, wonach durch die Schaffung des IT-Grundrechts der Schutzumfang der informationellen Selbstbestimmung nicht auf weitere Schutzdimensionen ausgedehnt wird, sondern dieser nötige und weitergehende Schutz in der grundrechtlichen Konkretisierung des IT-Grundrechts über strengere Anforderungen verwirklicht wird.

487 *Hauck* in: LR-StPO, § 100a StPO, Rn. 103 f.

aa) Begriffsverständnis im Sinne des § 100a Abs. 1 S. 2, 3 StPO

Teilt man den Begriff des informationstechnischen Systems in die beiden begrifflichen Einzelteile, so muss es sich bei einem System um eine Einheit technischer Anlagen handeln, die einer gemeinsamen Funktion dienen. Unter Informationstechnik ist die elektronische Informations- und Datenverarbeitung zu verstehen, womit sowohl Vorgänge der Kommunikation als auch solche der Datenverarbeitung umfasst sind.[488] Im Zuge einer systematischen und im Lichte des § 100a StPO erfolgten Auslegung wird vorgeschlagen, den Begriff des informationstechnischen Systems § 100a Abs. 1 S. 2 und 3 StPO ebenfalls kommunikationsbezogen auszulegen. Das informationstechnische System müsste daher konkret zu Kommunikationszwecken herangezogen werden.[489] Dieser Versuch einer Einengung des Begriffs wirkt in gewisser Weise gekünstelt und ist in Anbetracht dessen, dass § 100a Abs. 1 S. 2 StPO ohnehin nur für die Aufzeichnung von Kommunikationsvorgängen herangezogen werden darf auch inhaltsleer. Aufgrund dieser Voraussetzung wird ein informationstechnisches System ohnehin nur Ziel etwaiger Ermittlungsmaßnahmen sein, wenn sich hiervon Kommunikationsinhalte erhofft werden. Zwangsläufig weist das System sodann einen Telekommunikationsbezug auf, sodass diese zusätzliche Beschränkung auf Ebene des informationstechnischen Systems nicht erforderlich ist. Der Begriff ist vielmehr im Einklang mit seinem Wortlaut rein technisch zu verstehen. Das Endgerät zur Nutzung eines Sprachassistenten stellt daher aufgrund der verbauten Hard- und Software mitsamt der Technik zur Übertragung an die Serverzentren und der damit einhergehenden Datenverarbeitung in Form der Übermittlung ein informationstechnisches System dar.

bb) Server des Dienstleistungsanbieters als informationstechnisches System

Sofern sich die Daten nicht auf der lokalen Hardware befinden, sondern ein Zugriff auf die Server des Dienstleistungsanbieter erforderlich ist, ist fraglich, ob es sich auch bei diesem Server um ein informationstechnisches System handelt. Auf den ersten Blick scheint dies zuzutreffen, schließlich handelt es sich bei einem Server um ein hochkomplexes System, auf

488 Vgl. zum Ganzen *Hauck* in: LR-StPO, § 100a StPO, Rn. 105.
489 *Hauck* in: LR-StPO, § 100a StPO, Rn. 107.

welchem zudem die eigentliche Datenverarbeitung stattfindet. Dennoch könnte in Anbetracht der geplanten Infiltration eines Servers an eine Reduktion des Begriffs „informationstechnisches System" zu denken sein.[490] Für eine solche Erforderlichkeit streite, dass die kryptografischen Schlüssel zur Entschlüsselung stets nur den kommunizierenden Parteien bekannt sein dürften und die Dienstleistungsanbieter nicht dazu gezwungen werden dürften, den Schlüsselaustausch einer sich aufbauenden Verschlüsselung zu beeinträchtigen, wodurch sie selbst die bei der Nutzung ihres Systems garantierte Verschlüsselung der Nachrichtenübermittlung umgehen würden.[491] Dass die Unternehmen so ihre eigene geheimen Verschlüsselungen entschlüsselbar machen würden, stehe im Widerspruch zu den Eckpunkten deutscher Kryptopolitik.[492] Diese Kritik vermag jedoch nicht zu überzeugen. Ob die Strafverfolgungsbehörden die Daten vor der Verschlüsselung am Gerät des Betroffenen oder nach erfolgter Übertragung und Entschlüsselung aus den Servern ableiten ist sowohl hinsichtlich der Eingriffsintensität als auch hinsichtlich praktischer Folgen für den betroffenen Bürger ohne Unterschied. Es obliegt dem Staat hinsichtlich der gewonnenen Schlüssel mit der notwendigen Vorsicht zu agieren, sodass die Server des infiltrierten Dienstleistungsanbieters nicht durch unbefugte Dritte ebenfalls ausgelesen werden können. Das Bestehen einer solchen praktischen Gefahr kann jedoch nichts an der Möglichkeit ändern, auch auf Cloud-Server als informationstechnisches System zugreifen zu können. Entsprechend hat auch das BVerfG die Cloud als informationstechnisches System i.S.d. des § 20k Abs. 1 BKAG a.F. anerkannt.[493]

4) Ergebnis

Zwar sind sowohl das Endgerät als auch der Sprachassistent als informationstechnisches System im Sinne des § 100a Abs. 1 S. 2 StPO einzuordnen und damit grundsätzlich einer Quellen-Telekommunikationsüberwachung zur Umgehung einer Datenverschlüsselung zugänglich. Um unter Wahrung des Gesetzesvorbehalts im Rahmen der Quellen-Telekommunikationsüberwachung Daten abzufangen, müssten jedoch auch die übrigen

490 *Hauck* in: LR-StPO, § 100a StPO, Rn. 114; *Chaos Computerclub*, Stellungnahme, S. 18 f.
491 *Chaos Computerclub*, Stellungnahme, S. 18.
492 *Chaos Computerclub*, Stellungnahme, S. 18.
493 BVerfGE 141, 220, Rn. 209.

Voraussetzungen der Ermächtigungsgrundlage erfüllt sein. Zur rechtmäßigen Anordnung der Maßnahme müsste daher stets Telekommunikation im Sinne des § 100a StPO vorliegen. Nach zutreffendem strafprozessualem Begriffsverständnis ist dies bei der Nutzung eines Sprachassistenten jedoch nicht der Fall, sodass auch § 100a Abs. 1 S. 2 StPO als Ermächtigungsgrundlage ausscheidet.

III) § 100a Abs. 1 S. 3 StPO n.F.

1) Allgemeines

Eine im Kontext des § 100a StPO nicht zu erwartende Vorschrift wurde durch das am 24.08.2017 in Kraft getretene Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens in Form des § 100a Abs. 1 S. 3 StPO eingefügt.[494] Damit können nun auch auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Neben dem naheliegenden Fall des Zugriffs auf die Hardware des Endgeräts des betroffenen Nutzers, stellt sich zudem die Frage, ob über § 100a Abs. 1 S. 3 StPO auch die Daten nach erfolgter Entschlüsselung und Speicherung auf dem Server des Dienstleistungsanbieters abgegriffen werden könnten. Für ein solches Vorgehen gegen den Dienstleistungsanbieter müsste dieser als Betroffener angesehen werden. Betroffener in § 100a Abs. 1 S. 3 StPO könnte grundsätzlich auf zwei verschiedene Arten zu verstehen sein. Zum einen könnte mit Betroffener der Beschuldigte gemeint sein, gegen den Erkenntnisse gesammelt werden sollen und der daher vom Ergebnis der Erkenntnissammlung „betroffen" ist. Zum anderen könnte der Betroffene auch sein, in wessen Rechte die Zwangsmaßnahme eingreift. Für diesen Fall könnte Betroffener eines Eingriffs sowohl der Absender und Empfänger als auch der Dienstleistungsanbieter sein. Eine Antwort auf diese Frage gibt das Gesetz letztlich selbst: § 100a Abs. 3 StPO bestimmt, dass sich eine Maßnahme gegen den Beschuldigten sowie unter bestimmten Voraussetzungen auch gegen einen Nichtbeschuldigten richten könne. Von dem Nichtbeschuldigten müsste zu erwarten sein, dass er für den Beschuldigten bestimmte oder

494 Vgl. BGBl. 2017 I 3202.

von ihm herrührende Mitteilungen entgegennimmt oder weitergibt oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt. Für die Nutzung eines Sprachassistenten von Bedeutung ist dabei die letzte Alternative der Nutzung eines informationstechnischen Systems. Insofern könnte der Nutzer indem er an den Sprachassistent Befehle erteilt diesen als informationstechnisches System nutzen, welches der Dienstleistungsanbieter zur Verfügung stellt. In diesem Fall könnten die Strafverfolgungsbehörden auf die dort gespeicherten Informationen nach deren Entschlüsselung zugreifen. Sowohl in diesem Fall als auch beim Zugriff auf die Hardware vor Ort wäre jedoch weitere Voraussetzung, dass diese Kommunikation auch während des laufenden Übertragungsvorgangs aufgezeichnet werden dürfte. Unter Zugrundelegung des vorzuziehenden personell-individuellen Telekommunikationsbegriffs wäre dies jedoch wie gesehen nicht möglich, sodass sich an dieser Stelle, weitere Ausführungen erübrigen.

2) Verfassungsmäßigkeit der Vorschrift

Sofern die Rechtsprechung jedoch einem technikorientierten Kommunikationsverständnis zugeneigt ist und daher die Nutzung eines Sprachassistenten unter § 100a Abs. 1 StPO fassen müsste, würde ein Zugriff nach § 100a Abs. 1 S. 3 StPO in Betracht kommen. Gegen diese neu gefasste Vorschrift und damit auch gegen den sich auf § 100a Abs. 1 S. 3 StPO stützenden Zugriff müssen jedoch erhebliche verfassungsrechtliche Bedenken erhoben werden.

a) Keine Begrenzung auf laufende Telekommunikation

Im Unterschied zu § 100a Abs. 1 S. 1 StPO, der den Zugriff auf unverschlüsselte bzw. im Falle des § 100a Abs. 1 S. 2 StPO auf verschlüsselte Kommunikation erlaubt, rechtfertigt § 100a Abs. 1 S. 3 StPO einen weitergehenden Zugriff auch auf bereits vergangene und damit abgeschlossene Kommunikationsinhalte, deren Übertragungsvorgang bereits vollständig abgeschlossen ist und die auf einem hierzu benutzten informationstechnischen System gespeichert sind.[495] Insofern ist jedoch zu beachten, dass nach der Auffassung des BGH auch § 100a Abs. 1 S. 1 StPO einen Zugriff

495 *Bruns* in: KK-StPO, § 100a StPO, Rn. 44.

auf bereits ruhende Kommunikationsinhalte außerhalb eines Kommunikationsvorgangs rechtfertige, sofern diese nicht im alleinigen Herrschaftsbereich des Betroffenen gespeichert sind.[496] Im Übrigen stehen § 94 StPO und § 100a StPO in keinem Exklusivitätsverhältnis, sodass es unschädlich sei, dass das BVerfG in seiner IMAP-Entscheidung[497] entschied, dass beim Provider gespeicherte E-Mails auch mit der offenen Maßnahme des § 94 StPO beschlagnahmt werden können.[498] Ein Zugriff auf ruhende Kommunikationsdaten über § 100a StPO sei daher unter der genannten Voraussetzung auch wegen der im Vergleich zur Beschlagnahme deutlich strengeren Anforderungen im Wege eines Erst-Recht-Schlusses zulässig.[499] Die fehlende Begrenzung hinsichtlich laufender Kommunikation dürfte aus Sicht des BGH im Rahmen des § 100a Abs. 1 S. 3 StPO daher unschädlich sein. Gleichwohl ist kritisch zu sehen, dass § 100a Abs. 1 S. 3 StPO der Verwässerung des in der StPO tradierten Regelungskonzept Vorschub leistet. Von den Grundsätzen dieses Regelungskonzeptes ausgehend sollte § 100a Abs. 1 S. 1 und S. 2 StPO eine Eingriffsermächtigung für die heimliche Überwachung laufender Kommunikation darstellen. Diesen Ausgangsgedanken des historischen Gesetzgebers weichte der BGH bereits in der o.g. Entscheidung auf. Dagegen sollte die heimliche Durchsuchung ruhender – sich außerhalb eines Kommunikationsvorgangs – befindlicher Daten unter den Regelungsgehalt des § 100b StPO mitsamt dessen strengeren Voraussetzungen fallen.

---

496 BGH, NJW 2021, 1252, 1554; BGH, NJW 2009, 1828.

497 BVerfGE 124, 43 ff.

498 BGH, NJW 2021, 1252, 1554. Insofern wies auch bereits das BVerfG auf die bestehenden verschiedenen Möglichkeiten eines Zugriffs auf solche Daten nach § 94 StPO oder § 100a StPO hin, ohne dies jedoch abschließend zu bewerten, vgl. BVerfGE 124, 43, 60.

499 BGH, NJW 2021, 1252, 1554: kritisch zu dieser Begründung vgl. *Grözinger*, NStZ 2021, 358 f.; *Hiéramente* WiJ 2021, 19, 21 f. Der durch den BGH vorgenommene Erst-Recht-Schluss, komme vor dem Hintergrund des gänzlich unterschiedlichen Regelungsgehalts des § 94 StPO (Beschlagnahme) und des § 100a StPO (Überwachung) nicht in Betracht. Im Übrigen ist lediglich aufgrund des insofern zustimmungswürdigen Umstandes, dass die §§ 94 StPO und 100a StPO in keinem Exklusivitätsverhältnis stehen noch nicht gesagt, dass eine Ermittlungsmaßnahme nach § 100a Abs. 1 S. 1 StPO auch solche E-Mails umfasst, die zum Zeitpunkt des Zugriffs bereits versandt oder empfangen wurden, aber noch beim Provider gespeichert sind. Die Beantwortung dieser Frage richtet sich einzig nach den konkreten tatbestandlichen Voraussetzungen der Ermächtigungsgrundlage, vgl. zutreffend *Trüg*, JZ 2021, 560, 564. Vgl. hierzu auch oben Fn. 401.

b) Verstoß gegen die Maßstäbe des IT-Grundrechts

Wenig überraschend rückt die Vorschrift durch den Zugriff auf Vergangenes besonders in den Dunstkreis der Online-Durchsuchung nach § 100b StPO. Aus technischer Sicht kann diese Form der Quellentelekommunikationsüberwachung bereits nicht mehr von einer Online-Durchsuchung unterschieden werden. In dem einen wie dem andern Fall erfolgt eine Infiltration des Zielsystems zur Scannung sämtlicher gespeicherter Inhalte und damit ein Eingriff in die Integrität und Vertraulichkeit informationstechnischer Systeme. Trotz dieser Gleichheit mit § 100b StPO dürfen die Daten bei Heranziehung des § 100a Abs. 1 S. 3 StPO unter den niedrigeren Voraussetzungen des § 100a StPO ausgelesen werden.[500] Möglicherweise steht der neu eingefügte § 100a Abs. 1 S. 3 StPO diesbezüglich in einem Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts hinsichtlich des IT-Grundrechts. Wie gesehen soll nicht die Infiltration eines jeden IT-Systems vom Schutzbereich des Grundrechts umfasst sein, sondern nur solche, die eine Datenfülle aufweisen, die einen tiefen Einblick in die persönlichen Lebensverhältnisse des Einzelnen gewährt.[501] Ferner müssen die Daten einen Persönlichkeitsbezug aufweisen und in der Vertraulichkeit auf Geheimhaltung preisgegeben worden sein.[502] Eine solche erhebliche Datenmenge wie für die Einschlägigkeit des IT-Grundrechts erforderlich, wird nur dann betroffen sein, wenn gerade auch auf Daten zugegriffen wird, die über einen längeren Zeitraum gespeichert und somit für die Zukunft konserviert wurden. Auch auf solche konservierten Daten soll über § 100a Abs. 1 S. 3 StPO zugegriffen werden. Aufgrund der umfangreichen betroffenen Datenmengen, die nicht nur den aktuellen Kommunikationsinhalt wiedergeben, sondern auch sämtliche in der Vergangenheit liegende Kommunikationsinhalte offenbaren, darf der Zugriff hierauf nur nach Maßgabe des strengeren § 100b StPO erfolgen. Dies gilt jedoch nur, sofern die Daten im alleinigen Herrschaftsbereich des Betroffenen gespeichert sind. So führt das BVerfG in seiner Entscheidung zur Online-Durchsuchung aus, dass ein Eingriff dann nicht mehr an Art. 10 GG zu messen ist, wenn die Daten nach Abschluss eines Kommunikationsvorgangs im alleinigen Herrschaftsbereich[503] eines Kommunikati-

500 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 9.
501 BVerfGE 120, 274, 314.
502 *Luch*, MMR 2011, 75, 75.
503 Um einen solchen alleinigen Herrschaftsbereich handelt es sich nicht im Falle eines E-Mail-Postfachs, auf das der Nutzer nur über eine Internetverbindung

onsteilnehmers verbleiben und dieser geeignete Schutzmaßnahen gegen einen Zugriff treffen kann.[504] Sofern jedoch die in der Folge einer Infiltration bewirkten spezifischen Gefährdungen der Persönlichkeit durch ein Zugriff auf einen kompletten Datenspeicher durch Art. 10 Abs. 1 GG nicht hinreichend begegnet werden können und daher ein Schutz durch das neu geformte IT-Grundrecht von Nöten ist[505], kann der Eingriff in dieses Grundrecht, welches gerade den erhöhten Gefährdungen Rechnung tragen soll, konsequenterweise nicht auch unter den gleichen Voraussetzungen des § 100a StPO erfolgen, die bereits für einen Eingriff in Art. 10 GG maßgeblich sind. Ansonsten würde eben jene höhere Gefährdung für persönlichkeitsrelevantere Informationen faktisch überhaupt nicht zum Ausdruck kommen. Es ist nicht zu erklären, weshalb Inhalte, die zwar während des Übermittlungsvorgangs gem. § 100a Abs. 1 S. StPO hätten abgegriffen werden können, sodann aber auf einem informationstechnischen System gespeichert bleiben, das dem *alleinigen* Macht- und Herrschaftsbereich des Betroffenen unterfällt, gleichwohl nach § 100a Abs. 1 S. 3 StPO abgreifbar sein sollen. Obwohl diese Daten nach § 100a Abs. 1 S. 3 StPO nicht während eines unsicheren Übertragungsweges oder auf einen fremdbeherrschten Speicherplatz abgegriffen werden und sie daher bei einer entsprechenden Persönlichkeitsrelevanz dem IT-Grundrecht unterfallen, kann der Eingriff unverständlicherweise nach den milderen Voraussetzungen des § 100a StPO erfolgen.

c) Verhältnismäßigkeit hinsichtlich des Straftatenkatalog

Dass § 100a StPO im Vergleich zu § 100b StPO eine deutlich niedrige Eingriffsschwelle besitzt, zeigt sich an diversen Punkten. So wird bereits bei einem Vergleich der jeweils in Absatz 2 aufgeführten Katalogtaten deutlich, dass für § 100a StPO im Verhältnis zu § 100b StPO bereits vermeintliche Bagatelldelikte genügen, um eine Anordnung nach § 100a StPO zu erteilen. So genügt für eine Anordnung nach § 100a StPO beispielsweise bereits der Anfangsverdacht hinsichtlich einer Bestechlichkeit und

zugreifen kann. Dieses unterfällt weiterhin dem Schutzbereich des Art. 10 GG, vgl. BVerfGE 124, 43, 54 f.; BGH NJW 2021, 1252, 1254. Anders ist dies dann, wenn die E-Mails ausschließlich auf dem Endgerät des Betroffenen gespeichert sind.

504 BVerfGE 120, 274, 307 f.

505 BVerfGE 120, 274, 309.

Bestechung von Mandatsträgern nach § 108e StGB oder Delikte aus der Abgabenordnung nach § 100a Abs. 2 Nr. 2 StPO. Die Möglichkeit bereits beim Vorliegen solcher Delikte von vergleichsweise untergeordneter Bedeutung in das IT-Grundrecht eingreifen zu können, widerspricht der Rechtsprechung des Bundesverfassungsgerichts, wonach Eingriffe in das IT-Grundrecht nur der Verfolgung von Straftaten dienen dürfen, die ein überragend wichtiges Rechtsgut schützen.[506] Hierzu zählen Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren.[507] Diesen Maßstäben genügt der Katalog des § 100a StPO freilich nicht, der bereits das bloße Vermögen, das Vertrauen in die staatliche Verwaltung oder die Integrität des Sports als schützenswertes Rechtsgut beinhaltet. Dass die in § 100a StPO und § 100b StPO aufgezählten Straftaten von unterschiedlichem Gewicht sind, zeigt sich zudem darin, dass § 100b Abs. 1 StPO von „besonders schweren" Straftaten spricht, während in § 100a Abs. 1 StPO lediglich von „schweren" Straftaten die Rede ist.

d) Erhöhte Eingriffsintensität

Dass auch dieser Unterschied im Zuge der Gesetzgebung durchaus bemerkt wurde, zeigt der Versuch, den neu gefassten § 100a Abs. 1 S. 3 StPO durch die Darstellung des Zugriffs nach Satz 3 als „funktionales Äquivalent"[508] zur herkömmlichen Telekommunikationsüberwachung zu rechtfertigen. Als funktionales Äquivalent soll die neue Befugnis deshalb zu verstehen sein, da durch diverse Schutzvorrichtungen sichergestellt werden soll, dass lediglich Telekommunikation vernommen wird, die als laufende Telekommunikation auch über § 100a Abs. 1 S. 1, 2 StPO hätte erhoben werden können.[509] An eben diesen Schutzvorrichtungen äußerten Sachverständige bereits vor einigen Jahren erhebliche Bedenken. Es sei technisch überhaupt nicht möglich auszuschließen, dass bei der Infiltration eines kompletten Systems tatsächlich nur entsprechende Kommunikationsdaten erhoben würden.[510] Selbst wenn man von der Wirksamkeit

506 BVerfGE 120, 274, 326.
507 BVerfGE 120, 274, 328.
508 Ausschuss-Drucksache 18(6)334, S. 20.
509 Ausschuss-Drucksache 18(6)334, S. 21.
510 BVerfGE 120, 274, 309.

dieser Einschränkungen ausginge, müsste unter Heranziehung der Rechtsprechung des Bundesverfassungsgerichts die Äquivalenz zwischen § 100a Abs. 1 S. 1, 2 StPO und § 100a Abs. 1 S. 3 StPO verneint werden. Als Frage der Gesetzesanwendung, nicht aber der Gesetzesgültigkeit[511], ist § 100a Abs. 1 S. 3 StPO möglicherweise auf schlicht funktionaler Ebene und unter einer ergebnisorientierten Betrachtungsweise ein entsprechendes Äquivalent zu § 100a Abs. 1 S. 1, 2 StPO, jedoch keinesfalls hinsichtlich der damit einhergehenden Eingriffsintensität.[512] Durch die Infiltration des gesamten Systems um dieses auch komplett zu durchleuchten, wird die Eingriffsintensität der einfachen Telekommunikationsüberwachung und auch der Quellentelekommunikationsüberwachung um ein Vielfaches überstiegen. Dies gründet neben dem Eindringen des Staates in den von der Außenwelt abgeschiedenen Hoheitsbereich auf einem weiteren informationstechnischen Argument. Die praktische Umsetzung der gesetzgeberisch angedachten Einschränkungen, dass lediglich Daten über Kommunikationsinhalte, die in zeitlicher Hinsicht nach der richterlichen Anordnung stattfanden, erfasst werden sollen, intensiviert den staatlichen Eingriff weiter. Um diese Prüfung überhaupt durchführen zu können, ist es erforderlich, dass der eingesetzte Trojaner zunächst alle gespeicherten Inhalte ausliest und auswertet, um sodann zu entscheiden, ob es sich um Telekommunikationsinhalte handelt, die auch in zeitlicher Hinsicht unter Beachtung des § 100a Abs. 5 Nr. 2 StPO durch § 100a Abs. 1 S. 3 StPO erhoben hätten werden dürfen.[513] Bereits dieser Schritt stellt allerdings eine dem Staat zurechenbare Kenntnisnahme und mithin eine durch den Staat erfolgte Online-Durchsuchung dar. Da es jedoch auch bei anderen Überwachungsmaßnahmen durchaus der Fall sei, zunächst den Gesamtbestand an Kommunikation zu überprüfen, bevor in einem weiteren Schritt nicht verwertbare Inhalte (z.B. wegen des Kernbereichsschutzes) ausgesondert werden, soll es sich bei der bloßen Analyse der Meta-Daten mittels der eingesetzten Software um keine Online-Durchsuchung handeln.[514] Allerdings

511 BVerfGE 141, 220, Rn. 234.

512 Siehe auch *Grözinger*, Die Überwachung von Cloud-Storage, S. 300.

513 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 17. Im Vergleich zum Fall des § 100a Abs. 1 S. 3 StPO ist der entscheidende Unterschied, dass der eingesetzte Trojaner im Rahmen des § 100a Abs. 1 S. 2 StPO gerade diesen Zwischenschritt nicht erbringen muss. Dort müssen keine ruhenden Daten danach untersucht werden, ob es sich bei Ihnen um Kommunikation handelt auf die zugegriffen werden könnte, sondern lediglich alle aktuell ausgehenden Daten vor deren Verschlüsselung ausgeleitet werden.

514 *Kraus*, Stellungnahme, S. 8.

liegt bereits durch die für eine Maßnahme nach § 100a Abs. 1 S. 3 StPO erforderliche Infiltration und kompletten Scannung des Systems und der damit einhergehenden Gefährdungssituation für die gesamten Daten des Betroffenen eine Online-Durchsuchung vor. Dass dabei der konkrete Inhalt der kontrollierten Daten noch nicht unmittelbar durch menschliche Personen erfasst wird, ist an dieser Stelle nicht von Bedeutung. Erfasst werden schließlich die Metadaten, die in Anbetracht ihrer Menge, die sich wiederum dadurch ergibt, dass durch § 100a Abs. 1 S. 3 StPO auf den gesamten Datenbestand zugegriffen werden muss, ebenso Rückschlüsse auf die Persönlichkeit des Betroffenen zulassen können und somit ebenfalls vom IT-Grundrecht erfasst sind. Zudem verkennt der Vergleich mit dem Kernbereichsschutz und der dabei erforderlichen Überprüfung des Gesamtdatenbestands, dass es hier auf einer früheren Stufe – vor Fragen der tatsächlichen Beweiserhebung- oder Beweisverwertbarkeit – um die Frage nach einer überhaupt tauglichen Eingriffsbefugnis hierzu geht. In diesem Kontext sind Argumente aus dem Bereich des Kernbereichsschutzes nicht dienlich. Der Vergleich hinkt daher und ist nicht zielführend. Vielmehr soll durch ein Vorgehen nach § 100a Abs. 1 S. 3 StPO lediglich mittels einer Online-Durchsuchung durch die Hintertür ausfindig gemacht werden, auf welche Daten sodann unter dem Schein der Gesetzeskonformität durch § 100a Abs. 1 S. 3 StPO zugegriffen werden kann.

Hinzu kommt, dass die gesetzgeberische Argumentation, dass es sich bei § 100a Abs. 1 S. 3 StPO um ein bloßes funktionales Äquivalent handle[515], auch aus einem weiteren Punkt fehlgeht. Wenn es der Gesetzgeber aufgrund der Ähnlichkeit sowie der hypothetisch bestandenen Möglichkeit auf diese Informationen sowieso hätte zugreifen zu können, auch bei früherer Kommunikation „*verfassungsrechtlich nicht [für] geboten [erachtet], die wegen der besonderen Sensibilität informationstechnischer Systeme [...] aufgestellten höheren Anforderungen des Bundesverfassungsgerichts [für Eingriffe in das IT-Grundrecht] anzuwenden*“[516], verkennt dies die Systematik des § 100a StPO. Bereits die in § 100a Abs. 1 S. 2 StPO eingefügte Quellentelekommunikationsüberwachung stellt eine Ausnahme dazu dar, dass der Einsatz eines Trojaners zur Infiltration eines Systems eigentlich nur unter den Voraussetzungen des § 100b StPO möglich ist.[517] Das Vorgehen der Bundesregierung erweckt jedoch den Anschein, als wolle sie eine bestehende Ausnahme im selbem Atemzug um eine weitere Ausnahme erweitern.

515 Ausschuss-Drucksache 18(6)334, S. 20.
516 Ausschuss-Drucksache 18(6)334, S. 20.
517 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 16.

Dabei können Ausnahmen ihrem Sinn nach „*gerade nicht analog angewendet werden, sondern sind restriktiv auszulegen*".[518]

e) Zwischenergebnis

Bei der Infiltration eines informationstechnischen Systems, auf welchem der Betroffene Kommunikationsdaten- und Inhalte gespeichert hat, die in seiner alleinigen Herrschaftssphäre stehen, ist, aufgrund des Zugriffs auf den kompletten Datenbestand, ein Eingriff in das neu geschaffene IT-Grundrecht anzunehmen. Ein solcher Eingriff kann nicht unter Heranziehung des § 100a Abs. 1 S. 3 StPO legitimiert werden. § 100a StPO kann beim Vorliegen seiner Voraussetzungen von vornherein lediglich Eingriffe in das Fernmeldegeheimnis aus Art. 10 GG und das aus dem allgemeinen Persönlichkeitsrecht entspringende Recht auf informationelle Selbstbestimmung legitimieren. Aus den dargelegten Gründen ist § 100a Abs. 1 S. 3 StPO, der diese verfassungsrechtliche Differenzierung mitsamt der Systematik der §§ 100a ff. StPO, missachtet, verfassungswidrig.

IV) Überwachung eines Sprachassistenten als Minusmaßnahme zu § 100a StPO

Vereinzelt wird in der Literatur die Frage aufgeworfen, ob eine Maßnahme, die nicht unter eine entsprechende Ermächtigungsgrundlage subsumiert werden kann, als sog. Minusmaßnahme dennoch zulässig sei.[519] Voraussetzung hierfür wäre, dass die Überwachung eines Sprachassistenten als eine im Vergleich zum klassischen Fall der Telekommunikationsüberwachung mildere Maßnahme klassifiziert werden kann. Würde man dies beispielsweise für die Überwachung des Surfverhaltens im Internet andenken, so wäre zu konstatieren, dass die Überwachung des Surfverhaltens keineswegs eine mildere, sondern vielmehr eine einschneidendere Maßnahme als die herkömmliche Telekommunikationsüberwachung darstellt.[520] Durch

518 Stellungnahme des Deutschen Anwaltvereins zu dem Gesetzentwurf der Bundesregierung – Drs.18/11272, S. 11; abrufbar unter: https://anwaltverein.de/de/newsroom/sn-44-17-einfuehrung-der-online-durchsuchung-und-quellen-tkue?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2017/DAV-SN_44-17_%C3%84nderungsantrag.pdf (zuletzt abgerufen am 31.10.2021).

519 *Braun*, jurisPR-ITR 18/2013 Anm. 5; *Albrecht*, jurisPR-ITR 14/2013 Anm. 4.

520 *Hiéramente*, StraFo 2013, 96, 101.

die Überwachung des Surfverhaltens würden Informationen von solcher Qualität zusammengetragen, die es ermöglichten, umfassende Persönlichkeitsprofile zu erstellen. Durch die Auswertung des Surfverhaltens ließen sich umfassende Rückschlüsse auf die Persönlichkeit hinsichtlich sozialer Aktivitäten, sexueller Vorlieben, dem Gesundheitszustand und ähnlichem zusammentragen, die oftmals in dieser Detailgenauigkeit nicht einmal engsten Freunden und Familienangehörigen bekannt sein dürften.[521] Die Überwachung der Netzaktivitäten über einen längeren Zeitraum kann zur Erhebung einer Masse an personenbezogenen Daten führen, die ausgewertet eine Eingriffstiefe in die Persönlichkeitsrechte der Betroffenen vergleichbar mit einer Online-Durchsuchung erreichen können.[522] Die Überwachung der Netzaktivitäten stellt damit eine die Grundrechte des Betroffenen erheblich einschränkende Maßnahme dar. Aufgrund der dargestellten Ähnlichkeit dieses Falles zur Nutzung eines Sprachassistenten sind die Wertungen übertragbar. Selbst wenn ein Großteil der persönlichkeitsrelevanten Informationsverschaffung noch nicht über einen Sprachassistenten abgewickelt werden sollte, sondern noch über den klassischen Weg mit Tastatur und Computer erfolgt, können Sprachassistenten dennoch für die exakt gleichen Aufgaben herangezogen werden.

V) § 100b StPO

Nach § 100b Abs. 1 StPO darf auch ohne Wissen des Betroffenen mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und daraus Daten erhoben werden, wenn der Verdacht besteht, dass der Betroffene Täter einer in Absatz 2 genannten besonders schweren Straftat sein könnte, diese Tat auch im Einzelfall schwer wiegt und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre. Durch eine Infiltration der im Gehäuse verbauten Software oder des Sprachassistenten in Form des Severs des Dienstleistungsanbieters, könnte ein Zugriff auf gespeicherte Daten unter den Voraussetzungen des § 100b StPO möglich sein. Im Unterschied zu § 100a StPO steht hier nicht die Erfassung etwaiger Kommunikationsvorgänge, sondern eine vollumfängliche Ausforschung des infiltrierten informationstechnischen Systems im Vordergrund. Eine erforderliche Ermäch-

521 *Hiéramente*, StraFo 2013, 96, 100 f.
522 BVerfGE 120, 274, 324 f.

tigung hierzu fand sich in der Strafprozessordnung gleichwohl über viele Jahre nicht. Erst im Jahr 2017 kam es im Zuge der Reform zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, zur Schaffung der heutigen Eingriffsbefugnis. Diese erlaubt, dass ohne Wissen des Betroffenen in ein von diesem benutzten informationstechnischen System eingegriffen wird und Daten erhoben werden. Vor Kodifizierung dieser Norm war den Ermittlungsbehörden nur der offene Zugriff auf „ruhende" Daten im Rahmen der Durchsuchungs- und Beschlagnahmevorschriften, §§ 94 ff., 102 ff. StPO möglich.[523] § 100b StPO ergänzt die Ermittlungsmaßnahmen um eine Möglichkeit des verdeckten Zugriffs. Obgleich des Unterschiedes zwischen offener und verdeckter Durchsuchung, wurde die verdeckte Online-Durchsuchung mit dem Argument, dass dem Ermittlungsverfahren kein Offenheitsgrundsatz zu Grunde läge, unter Heranziehung des § 102 StPO ehemals selbst durch den BGH akzeptiert.[524] Mit Beschluss vom 25.11.2006 stellte ein Ermittlungsrichter jedoch fest, dass die verdeckte Online-Durchsuchung mangels laufender Kommunikation nicht auf § 100a StPO, mangels eines offenen Zugriffs nicht auf § 102 StPO und aufgrund der hohen Eingriffsintensität auch nicht auf die Ermittlungsgeneralklausel gestützt werden kann.[525] Diese Sichtweise fand in der Folge Zustimmung, sodass eine verdeckte Online-Durchsuchung lange Zeit als unzulässig betrachtet wurde.[526]

Entscheidendes Abgrenzungsmerkmal der Online-Durchsuchung zur Telekommunikationsüberwachung ist daher grundsätzlich die Bewegung der Daten und die damit korrelierende Frage, ob sich diese hierdurch in der „freien Umlaufbahn" (mit der Konsequenz eines geringeren Schutzes) befinden oder im Hoheitsgebiet der Privatsphäre des Einzelnen ruhen und daher besonders geschützt sind.

1) Infiltration des Endgeräts

a) Möglichkeiten der Infiltration

Die hierfür notwendige Infiltration des betroffenen Systems ist auf verschiedenen Wegen durchführbar. Es ließen sich die Systeme bereits bei

523 *Brodowski*, JR 2009, 402, 411.
524 Vgl. BGH, StV 2007, 60, 61; *Hofmann*, NStZ 2005, 121, 123.
525 BGHSt 51, 211, 218.
526 *Cornelius*, JZ 2007, 798, 799; *Valerius*, JR 2007, 275, 277.

der Fertigung mit entsprechenden Funktionen oder Sicherheitslücken ausstatten. Es bestünde dann jedoch die Gefahr, dass solche Sicherheitslücken nicht nur durch die Strafverfolgungsbehörden, sondern auch durch Unbefugte Dritte ausgenutzt würden. Auch die Gesetzesbegründung legt nahe, dass die Systeme nachträglich mit einem entsprechenden Programm infiltriert werden sollen.[527] Die nachträgliche Infiltration lässt sich in zwei verschiedene Möglichkeiten unterscheiden. Möglich ist zum einen ein physischer Zugriff auf das System, wozu die Wohnung betreten und die benötigte Software auf dem zu durchsuchenden System installiert wird.[528] In diesem Fall müsste § 100b StPO allerdings zum Betreten der Wohnung ermächtigen und damit einen Eingriff in Art. 13 GG rechtfertigen. Ausgehend von den Gesetzesmaterialien wird Art. 13 GG nicht als durch § 100b StPO einschränkbares Grundrecht genannt.[529] Daher wird zurecht angenommen, dass die Anordnung nach § 100b StPO nicht die Befugnis umfasst, die Wohnung des Betroffenen zum Zwecke der Infiltration des informationstechnischen Systems heimlich zu betreten.[530] Darüber hinaus ist eine Konstruktion dieser Befugnis über eine Annex-Kompetenz weder rechtlich zulässig noch erforderlich. Bei dem Betreten der Wohnung würde es sich um einen eigenständigen Grundrechtseingriff handeln, nicht jedoch um eine bloße Begleitmaßnahme der Online-Durchsuchung. Ferner stehen den Strafverfolgungsbehörden im Rahmen des § 100b StPO Möglichkeiten der Infiltration zur Verfügung, die Art. 13 GG nicht aufgrund des Zutritts zur Wohnung des Grundrechtsberechtigten tangieren.[531] Als ein solches Mittel ist hier ein Fernzugriff durch den Einsatz eines Staatstrojaner denkbar. Das Aufspielen eines solchen Trojaners könnte durch das Ausnutzen von unbemerkten Sicherheitslücken (sog. Zero-Day-Exploits) oder durch eine täuschende Manipulation des Nutzers, beispielsweise durch sog. Phishing, erfolgen, indem einem Nutzer infizier-

527 BT-Drs. 18/12785, S. 53.

528 *Soiné*, NStZ 2018, 497, 501; *Derin/Golla*, NJW 2019, 1111, 1112.

529 Vgl. *Soiné*, NStZ 2018, 497, Fn. 64.

530 ; *Soiné*, NVwZ 2012, 1585,1588 f., *ders*., NStZ 2018, 497, 501; *Derin/Golla*, NJW 2019, 1111,1112; *Singelnstein/Derin*, NJW 2017, 2646, 2647; *Graf* in: BeckOK-StPO, § 100a StPO, Rn. 117 auch hinsichtlich § 100a Abs. 1 S. 2 StPO; a.A. *Bruns* in: KK-StPO, § 100b StPO, Rn. 4, der eine Annexkompetenz bejaht, wenn keine anderen erfolgsversprechenden Möglichkeiten bestehen.

531 *Soiné*, NStZ 2018, 497, 500, der ferner davon ausgeht, dass von dem Verbot der heimlichen Wohnungsbetretung dann ausnahmsweise abgewichen werden könne, wenn außer einer Maßnahme nach § 100 b StPO zusätzlich eine Überwachung nach § 100c StPO besteht.

te Dateien übermittelt werden durch deren Öffnen sich das System selbst infiltriert.[532]

b) Infiltration des Endgeräts zur Online-Durchsuchung

Bei dem vom Betroffenen genutzten Endgerät handelt es sich zwar um ein informationstechnisches Gerät des Betroffenen im Sinne des § 100b StPO[533], jedoch sind in der Praxis auf der Software des Endgeräts in der Regel keine ruhenden Kommunikationsdaten gespeichert. Da eine solche Speicherung einen absoluten Ausnahmezustand darstellt, ist die Infiltration nach § 100b StPO zu direkten Informationsgewinnung von untergeordneter Bedeutung.

c) Infiltration des Endgeräts zur Online-Live-Überwachung

Von der Online-Durchsuchung kann begrifflich die Online-Überwachung, aber auch die Online-Live-Überwachung unterschieden werden. Während eine Online-Durchsuchung einen einmaligen punktuellen Zugriff auf die Daten eines informationstechnischen Systems umfasst, meint die Online-Überwachung eine Überwachung über einen bestimmten längeren Zeitraum.[534] Dabei besteht in Form der Online-Live-Überwachung für die Ermittlungsbehörden die Möglichkeit über das infiltrierte Endgerät ablaufende Aktivitäten in Echtzeit zu überwachen und so Kenntnis von gegenwärtig ablaufenden Vorgängen zu erhalten.[535] Noch zu klären ist, ob zur Ermöglichung einer solchen Live-Überwachung technische Funktionen des Endgeräts durch die Strafverfolgungsbehörden aktiviert werden dürfen, um den Verdächtigen mithilfe dieser Funktionen ausspähen zu können. Anerkannt ist dagegen die Möglichkeit, den Betroffenen durch kriminalistische List zur Nutzung und daher Aktivierung der Sensorik beispielsweise des Mikrofons des Sprachassistenten zu animieren.[536] Sodann können die Strafverfolgungsbehörden auf die durch das Endgerät aufge-

532 *Derin/Golla*, NJW 2019, 1111, 1112; *Soiné*, NStZ 2018, 497, 501 f.; *Blechschmitt*, StraFo 2017, 361, 362.
533 A.A.: *Graf* in: BeckOK-StPO, § 100b StPO, Rn. 11.
534 *Hornick*, StraFo 2008, 281, 282.
535 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 8.
536 *Soiné*, NStZ 2018, 497, 502.

zeichneten Audioaufzeichnungen zugreifen, indem sie die während des folgenden Übertragungsvorgangs übermittelten Daten ausleiten.

2) Zugriff auf Mikrofon und Kamera

Einer näheren Betrachtung zuzuführen, ist jedoch die Frage, ob die im Endgerät verbauten Komponenten über § 100b StPO auch zur mittelbaren Informationsgewinnung genutzt werden dürften. Es stellt sich daher die Frage, ob im Rahmen des § 100b Abs. 1 StPO auf Kamera oder Mikrofon des Endgeräts eines Sprachassistenten bzw. des Smart Speakers fremdgesteuert zugegriffen werden dürfte.[537] Aus technischer Sicht ist es ohne weiteres möglich, mittels der aufgespielten Überwachungssoftware auch eine vollumfängliche Raumüberwachung, beispielsweise durch eine Aktivierung des Mikrofons, der Kamera oder weiterer sensorischer Systeme des betroffenen Geräts, zu ermöglichen.[538] Wenngleich nach Angaben des Bundesinnenministeriums solche Maßnahmen zum jetzigen Stand nicht geplant sind,[539] fragt sich ob diese denn rechtlich überhaupt zulässig wären.

a) Wortlaut

Ausweislich des Wortlauts darf in ein informationstechnisches System eingegriffen werden, um daraus Daten erheben zu können. Unter Bezugnahme auf die Weite des Wortlauts, wird argumentiert, dass dieser einer Aktivierung der sensorischen Systeme des überwachten Geräts nicht entgegenstünde.[540] Sofern mittels dieser Instrumente Daten aus der Umgebung aufgefangen werden, würden diese schließlich im weitesten Sinne aus dem infiltrierten System gewonnen und an die Ermittlungsbehörden weitergeleitet.[541] Der Passus „dürfen Daten daraus erhoben werden“ ist jedoch

537 Erstmals zu dieser noch ungeklärten Frage *Rüscher*, NStZ 2018, 687, 690; mit bloßem Hinweis auf diese Fragestellung *Eschelbach* in: SSW-StPO, § 100b StPO, Rn. 4.

538 *Fox*, Stellungnahme, S. 8.

539 Fragenkatalog der SPD-Bundestagsfraktion, S. 13, vgl. https://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt abgerufen am 31.10.2021).

540 *Eschelbach* in: SSW-StPO, § 100b StPO, Rn. 4; *Weber;* jM 2021, 252, 255.

541 *Eschelbach* in: SSW-StPO, § 100b StPO, Rn. 4.

vielmehr so zu verstehen, dass über § 100b StPO lediglich Daten erhoben werden dürfen, die zum Zeitpunkt der Infiltration oder in deren Verlauf durch eine Handlung des Nutzers selbst auf diesem System gespeichert wurden.[542] Davon nicht umfasst ist, dass diese Daten nach der Infiltration in einem weiteren Schritt noch gewonnen werden müssen. Insofern ist mit dem Wortlaut der Norm also zu differenzieren, ob unmittelbar auf gespeicherte Daten zugegriffen werden kann oder ob dieser Zugriff nur mittelbar erfolgen könnte, da die Daten erst noch neu zu generieren wären.[543] Zweiteres wäre schließlich bei Sprachassistenten der Fall, da deren Kamera oder Mikrofon erst extern aktiviert werden müsste, um sodann mögliche Daten erheben zu können. Diese Form der mittelbaren Beweisgewinnung kann mit dem Wortlaut des § 100b Abs. 1 StPO nicht in Einklang gebracht werden. Dieser gestattet lediglich die direkte Erhebung der Daten aus dem System, nicht jedoch dessen manipulative Nutzung und Erhebung durch das System selbst.[544]

b) Historie

Sofern versucht wird die Norm aus einem historischen Blickwinkel zu betrachten, wird dies aufgrund ihrer erst kurzen Existenz keine Aufschlüsse liefern. Jedoch könnte mit Blick auf die Gesetzesbegründung anzunehmen sein, dass die Verwendung sensorischer Systeme vom Umfang der Norm umfasst sein soll. Ausweislich derer soll neben dem Zugriff auf gespeicherte Daten, auch ein Zugriff auf das gesamte Nutzerverhalten möglich sein.[545] Mit dem Verweis auf das gesamte Nutzungsverhalten war jedoch nicht die Aktivierung etwaiger Systeme durch die Strafverfolgungsbehörden, sondern eine sog. Live-Überwachung der Nutzung des Beschuldigten derart gemeint, dass die Behörden dem Nutzer „heimlich über die Schulter blicken" und so seine aktuellen Vorgänge verfolgen können.[546]

542 so auch Rüscher, NStZ 2018, 687, 691; *Roggan*, StV 2017,821, 826; *Großmann*, JA 2019, 241, 244; *Gercke* in: HK-StPO, § 100b StPO, Rn. 11; *Soiné*, NStZ 2018, 497, 502; *Brodowski* in: BeckOK-ITR, X, § 100b StPO, Rn. 5.

543 *Kruse/Grzesiek*, KritV 2017, 331, 345.

544 *Singelnstein/Derin,* NJW 2017, 2646, 2647; vom Gegenteil ausgehend wohl *Huber*, NVwZ 2007, 880, 883.

545 BT-Drs. 18/12785, S. 54.

546 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 5.

c) Systematik

In Anbetracht dessen, dass es sich bei der neu geschaffenen Befugnis um eine der eingriffsintensivsten Ermittlungsbefugnisse der StPO handeln soll und deren Voraussetzung an die der akustischen Wohnraumüberwachung aus § 100c StPO angelehnt seien,[547] könnte anzunehmen sein, dass sodann auch eine (akustische) Wohnraumüberwachung auf Grundlage des § 100b StPO möglich sein müsse. Verglichen mit den übrigen Ermittlungsbefugnissen findet im Gegensatz zu § 100a StPO und § 100c StPO, bei § 100b StPO nicht lediglich eine Überwachung der aktuellen Kommunikation, sondern vielmehr sämtlicher vergangener und laufender Daten auf dem betroffenen System statt. Wenn jedenfalls eine akustische Wohnraumüberwachung unter den Voraussetzungen des § 100c StPO angeordnet werden darf, dann müsse eine solche auch durch Einschaltung des Mikrofons unter den Voraussetzungen des § 100b StPO zulässig sein, auf dessen Straftatenkatlog § 100c StPO indes explizit verweist. Teilweise wird sogar behauptet, die neu geschaffene Online-Durchsuchung legitimiere sämtliche Eingriffe, die bisher auf Grundlage des § 100c StPO möglich waren.[548] Dem kann jedoch nicht gefolgt werden. Ungeachtet dessen, dass § 100c StPO dann praktisch ohne eigenständige Funktion wäre, sind § 100b StPO und § 100c StPO hinsichtlich ihrer Anordnungsvoraussetzungen gerade nicht gleich. Im Unterschied zu § 100b StPO ist für eine Anordnung nach § 100c Abs. 1 Nr. 3 StPO weiter erforderlich, dass auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind. Gemessen an den Eingriffsvoraussetzungen handelt es sich bei § 100b StPO mithin auch keineswegs um die schwerwiegendsten strafprozessuale Ermächtigungsgrundlage. Vielmehr bleibt es dabei, dass § 100c StPO die ultima ratio der heimlichen Ermittlungsmaßnahmen darstellt.[549] Hinzu kommt ein gewichtiger Unterschied zwischen § 100b und § 100c StPO. Während die Datenfülle, auf die unter den Voraussetzungen des § 100b StPO zugegriffen werden kann, sicherlich immens ist, gilt es bei einer Wohnraumüberwachung einen weiteren Aspekt zu bedenken. Gespräche in den eigenen vier Wänden finden tatsächlich vollkommen abgeschnitten von der Außenwelt statt. Eine Verbindung zur

547 *Singelnstein/Derin,* NJW 2017, 2646, 2647.
548 *Beukelmann*, NJW Spezial 2017, 440.
549 *Großmann*, GA 2018, 439, 442.

Außenwelt besteht nicht einmal – wie im Falle der Nutzung eines informationstechnischen Systems – durch die Inanspruchnahme etwaiger technischer Geräte. Während bei der Nutzung eines technischen Geräts permanent Spuren hinterlassen werden, ist es hinsichtlich eines Gesprächs in der eigenen Wohnung die „Flüchtigkeit des gesprochenen Wortes“[550], die im Zuge einer Wohnraumüberwachung mittels eines externen Eingriffs konserviert wird. Das Abhören und Speichern solcher Nachrichten ist im Kanon der Eingriffsbefugnisse der §§ 100a ff. StPO explizit der Wohnraumüberwachung nach § 100c StPO zugewiesen. Im Übrigen hätte der Gesetzgeber, sofern er sich für eine akustische oder visuelle Wohnraumüberwachung mit Hilfe der infiltrierten Geräte aussprechen wollte, dies durch einen Verweis auf § 100c StPO deutlich machen können.[551] Ein solcher Verweis ist ebenso nicht erfolgt, sodass eine Wohnraumüberwachung auch unter systematischen Gesichtspunkten nicht auf § 100b StPO gestützt werden darf.

Gegen eine aktive Aktivierung von Kamera und Mikrofon durch die Strafverfolgungsbehörden spricht ferner ein Vergleich mit den bereits seit längerer Zeit in diversen Landes- und Bundesgesetzten normierten Befugnissen zur Online-Durchsuchung mit präventiver Ausrichtung. Bereits hinsichtlich dieser polizeirechtlichen-präventiven Norm entwickelte das Bundesverfassungsgericht enge Zulässigkeitsvoraussetzungen[552]. Wenn bereits für präventive Maßnahmen, durch deren Hilfe der sich aus einer Gefahr entwickelnde Schaden noch verhindert werden könnte solch strenge Anforderungen gelten, dann muss dies erst recht für repressive Maßnahmen gelten, die „lediglich“ die Sanktionierung einer bereits eingetretenen Straftat ermöglichen sollen. Mit diesem engen Verständnis lässt sich dann aber nicht vereinbaren, den Wortlaut der Norm in seiner denkbar weitesten Form zu lesen. Eine historisch vergleichende Betrachtung legt daher ein enges Verständnis des Wortlauts nahe, was eine Aktivierung sensorischer Systeme des informationstechnischen Systems ausschließt.

550 BGHSt 57, 71, 75 ff.
551 *Rüscher*, NStZ 2018, 687, 691.
552 Sowohl in § 20k BKAG a.F. als auch in § 5 Abs. 2 Nr. 11 VSG NRW wurde die Online-Durchsuchung aufgrund ihrer Unbestimmtheit bzw. einer zu weiten Begriffsfassung durch das BVerfG für verfassungswidrig erklärt, vgl. BVerfGE 120, 274, 302 ff.; BVerfGE 141, 220, 304 ff.

d) Telos

§ 100b StPO soll der heimlichen Ausspähung eines technischen Systems dienen und dabei den Zugriff auf gespeicherte Daten ermöglichen. Auf diesem Wege sollen Informationen zur Aufklärung einer Katalogtat des § 100b Abs. 2 StPO heimlich ausgelesen werden. Ziel der Ermächtigungsgrundlage ist daher das Ausspähen eines informationstechnischen Systems, nicht aber eines Wohnraums. Dieses Ergebnis bestätigt auch Gesetzesbegründung, in der sich im Zusammenhang mit der Infiltration eines informationstechnischen Systems ausführlich mit möglichen Eingriffen in das IT-Grundrecht auseinandergesetzt wird, nicht aber mit einem möglichen Eingriff in Art. 13 GG.[553] Ein Eingriff in den Schutzbereich der Unverletzlichkeit der Wohnung liegt jedoch nahe, wenn dieser akustisch oder gar visuell überwacht wird. Der Gesetzgeber selbst spricht von der Beeinträchtigung des Art. 13 GG jedoch stets nur im Zusammenhang mit einem Vorgehen nach § 100c StPO.[554] Es sollte daher gerade nicht Sinn und Zweck des § 100b StPO sein, in die Privatsphäre der Wohnung einzudringen.

e) Zwischenergebnis

Es bleibt festzuhalten, dass die Aktivierung von Mikrofon oder Kamera infiltrierter Systeme nicht von § 100b StPO gedeckt ist. Die Nutzung dieser Instrumente wird dadurch jedoch nicht gänzlich ausgeschlossen. Ausgeschlossen ist lediglich die Aktivierung der Systeme seitens der Strafverfolgungsbehörden. Sofern jedoch das System infiltriert wurde und sich der Nutzer zur Verwendung der Kamera oder des Mikrofons entscheidet, können bei einer Live-Überwachung die dabei offenbarten Information über § 100b StPO abgegriffen werden.[555] Wird folglich ein infiltriertes Gerät vor Ort durch den Nutzer aktiviert und zeichnet das Mikrofon sodann ein Gespräch des Nutzers zur Weiterleitung an den Sprachassistenten auf, kann diese Kommunikation über § 100b StPO abgefangen werden. Offen bleibt damit die Frage nach der Verwertbarkeit eines auf diese Weise erlangten Beweises, worauf im weiteren Verlauf gesondert eingegangen werden soll.

553 BT-Drs. 18/12785, S. 48.
554 BT-Drs. 18/12785, S. 48.
555 *Brodowski* in: BeckOK-ITR, X, § 100c StPO, Rn. 7.

3) Infiltration der Server des Dienstleistungsanbieters

Daneben ist ebenso an eine Infiltration der Server des Dienstleistungsanbieters zu denken. § 100b StPO stellt eine allumfassende Eingriffsbefugnis dar,[556] die sich nicht darin erschöpft lediglich auf informationstechnische Systeme des Verdächtigen zuzugreifen. Unter den Voraussetzungen des § 100b Abs. 3 StPO kann auf die Cloud-Server des Dienstleistungsanbieter als „andere Person" zugegriffen werden, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte deren informationstechnisches System nutzt. Bei einer derartigen Maßnahme ist zudem zu beachten, dass nicht lediglich der Dienstleistungsanbieter als unbeteiligte Person betroffen ist, sondern mittelbar auch sämtliche weitere Personen, deren Daten aufgrund der Nutzung einer Dienstleistung des Anbieters ihre Daten auf dem infiltrierten Server speichern. § 100b Abs. 3 S. 2 StPO legitimiert lediglich den Zugriff auf das informationstechnische System einer anderen Person (des Dienstleistungsanbieters), wenn auf Grundlage bestimmter Tatsachen davon auszugehen ist, dass der Beschuldigte informationstechnische Systeme der anderen Person benutzt und der alleinige Zugriff auf sein eigenes informationstechnisches System nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts eines Mitbeschuldigten führen wird. Hinsichtlich der Frage, wie es sich auswirkt, dass auf diesem Server persönlichkeitsrelevante Daten von Millionen anderer Unbeteiligter Nutzer gespeichert sind, erlaubt § 100b Abs. 3 S. 3 StPO die Maßnahme auch dann auszuführen, wenn andere Personen unvermeidbar betroffen sind. Aus dem Einschub „unvermeidbar" ergeben sich hohe Anforderungen an die Verhältnismäßigkeit eines solchen Vorgehens. Praktisch wird diese Anforderung jedoch zu Recht als inhaltsleer bezeichnet. Vielfach werden vor der Anordnung Anhaltspunkten für eine sachgerechte Beurteilung fehlen. Die Verhältnismäßigkeitsprüfung wird sodann lediglich auf vagen Prognosen beruhen.[557] Dass die Drittbetroffenheit im konkreten Fall der Infiltration des Servers einen Dienstleistungsanbieters mit Kunden im dreistelligen Millionenbereich weltweit jedoch evident ist, dürfte keine vage Prognose darstellen. Insofern sind in diesen Fällen an die Verhältnismäßigkeitsprüfung – wenngleich der Gesetzgeber den Zugriff trotz Drittbetroffenheit grundsätzlich zulässt – tatsächlich hohe Anforderungen, vergleichbar mit denen der ultima ratio Klausel in § 100c Abs. 1 Nr. 4 StPO, zu stellen. Zudem ist im Falle der angedachten Sys-

556 *Grözinger*, StV 2019, 406, 411.
557 *Hauck* in: LR-StPO, § 100c StPO, Rn. 117.

teminfiltration beim unverdächtigen Dienstleistungsanbieter § 100b Abs. 1 Nr. 3 StPO besondere Bedeutung beizumessen. Die von den Ermittlungsbeamten erhofften Informationen werden beim Dienstleistungsanbieter in aller Regel auch mittels einer offenen Ermittlungsmaßnahme im Rahmen einer Durchsuchung und einer möglichen Beschlagnahme gesichert werden können.[558] Notwendig wäre eine heimliche Überwachung vielmehr dann, wenn ein Bekanntwerden der Überwachung den Ermittlungserfolg gefährden würde. Allerdings ist bei einem Dienstleistungsanbieter regelmäßig nicht zu befürchten, dass dieser Aufzeichnungen der Kunden zur Vereitelung eines Zugriffs löschen würden. Vielmehr haben die Dienstleistungsanbieter in der Praxis Kontaktstellen für behördliche Anfragen eingerichtet, die sodann mit den Behörden kooperieren.[559]

4) Verfassungswidrigkeit des § 100b StPO

a) Fehlende ultima-ratio Ausgestaltung

Auch die neu geschaffene Online-Durchsuchung sieht sich verfassungsrechtlichen Bedenken ausgesetzt. Diese gründen vor allem auf einem Vergleich mit § 100c StPO und dessen strengeren Voraussetzungen, wenngleich § 100b StPO für den schwerwiegenderen Grundrechtseingriff empfunden wird.[560] Es wird kritisiert, dass die Online-Durchsuchung im Unterschied zur akustischen Wohnraumüberwachung – nicht als ultima ratio ausgestaltet ist.[561] Während § 100b Abs. 1 Nr. 3 StPO fordert, dass ein Vorgehen auf andere Weise lediglich „wesentlich" erschwert sein müsse, muss ein Vorgehen auf andere Weise für eine Anordnung nach § 100c Abs. 1 Nr. 4 StPO „unverhältnismäßig" erschwert sein. Das Bestehen dieses Unterschieds wäre verfassungsrechtlich aber jedenfalls dann nicht zu beanstanden, wenn – entgegen teilweiser Stimmen in der Literatur – auch

558 Vgl. § 4, A., IX), 1).
559 *Gercke* in: Borges/Meents Cloud-Computing, § 20, Rn. 38.
560 *Singelnstein/Derin*, NJW 2017, 2646, 2647.
561 *Park*, Durchsuchung und Beschlagnahme, § 4, Rn. 838; vgl. die anhängige Verfassungsbeschwerde (AZ: 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18) gegen die Regelungen der Strafprozessordnung zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung beim Bundesverfassungsgericht, abrufbar unter: https://www.fdpbt.de/sites/default/files/2021-07/20210714_VfB_Pressefassung_0.pdf (zuletzt abgerufen am 31.10.2021).

nach Schaffung des § 100b StPO, weiter § 100c StPO den schwerwiegendsten Grundrechtseingriff darstellen würde. Hinsichtlich der Online-Durchsuchung ist zuzugeben, dass der Zugriff auf Vergangenes eine erhebliche Eingriffsintensität mit sich bringt. Dass solche Eingriffe die durch § 100c StPO legitimierten Eingriffe in die Unverletzlichkeit der Wohnung übersteigen, kann allerdings nicht ohne einhergehende Begründung behauptet werden.[562] *Buermeyer* begründet den schwerwiegenderen Eingriff durch § 100b StPO damit, dass durch eine akustische Wohnraumüberwachung zu erlangende Erkenntnisse auch im Wege einer Online-Durchsuchung generiert werden können, wenn das Mikrofon des Systems heimlich aktiviert wird.[563] Daraus folge, dass Online-Durchsuchung gegenüber dem Großen Lauschangriff „*ein – erhebliches – Plus, kein Aliud oder gar Minus*" darstelle.[564] Dieses Argument kann aber bereits deshalb nicht durschlagen, da wie gezeigt, der aktive Einsatz eines Mikrofons oder der Kamera unzulässig ist. Um die Eingriffsintensität eines Eingriffs nach § 100c StPO bestimmen zu können, sind ferner auch die bereits beschriebenen Charakteristika eines Gesprächs in der eigenen Wohnung zu beachten. Solche Gespräche werden im Vertrauen auf absolute Abgeschiedenheit und Isolation von etwaigen Dritten geführt. Es ist mittlerweile bekannt, dass die Nutzung eines informationstechnischen Geräts stets mit gewissen Risiken einhergeht und rückverfolgbare Spuren hinterlassen werden. Auch verfassungsrechtlich ist die eigene Wohnung seit jeher als Rückzugsort besonders privilegiert. Zum einen konkretisiert Art. 13 GG in seiner einfachgesetzlichen Ausgestaltung die Menschenwürdegarantie. Zum anderen beinhaltet Art. 13 GG neben diesem engen Bezug zur Menschenwürde das verfassungsrechtliche Gebot unbedingter Achtung einer Privatsphäre des Bürgers, die diesem eine höchstpersönliche Entfaltung ermöglicht.[565] Die in der eigenen Wohnung ablaufenden Gespräche sind alleine aufgrund dieses Umstands von vorherein mit dem Stempel der Privat- und Vertraulichkeit versehen. Für die Nutzung eines informationstechnischen Systems wiederum kann dies nicht in der gleichen allgemeingültigen Weise dargelegt werden. Dies zeigt bereits der Umstand, dass das Bundesverfassungsgericht nicht bei jeder Infiltration eines informationstechnischen Systems auch die Eröffnung des IT-Grundrechts für erforderlich hält. Bei Zugrundelegung dessen ist die pauschale Einordung, es handle sich bei der neu geschaffenen Online-

562 So jedoch *Singelnstein/Derin,* NJW 2017, 2646, 2647.
563 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 15.
564 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 15.
565 BVerfGE 109, 279, 313.

Durchsuchung um den schwerwiegendsten Eingriff der Strafprozessordnung, daher nicht haltbar.[566] Eine unterschiedliche Ausgestaltung des ultima ratio Gedankens ist daher verfassungsrechtlich nicht zu beanstanden und führt nicht zu einer Verfassungswidrigkeit der Vorschrift.

b) Unzureichende Ausgestaltung des Kernbereichsschutzes

Hinsichtlich der Ausgestaltung des Kernbereichsschutzes in § 100d Abs. 1 bis 3 StPO wird kritisiert, dass es dort an einem Beweiserhebungsverbot fehle, wie es § 100d Abs. 4 S. 2 StPO für den Fall des § 100c StPO normiere.[567] Danach ist das Abhören und Aufzeichnen unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Allerdings gestaltet sich die Online-Durchsuchung insofern wesensverschieden zur Wohnraumüberwachung. Wenn im Rahmen einer Wohnraumüberwachung Gespräche mitgehört werden, die dem Kernbereichsschutz unterfallen, können in diesem Moment faktisch keine weiteren Beweise erhoben werden. Die sofortige Unterbrechung der Abhörmaßnahme stellt daher die logische Konsequenz dar. Im Rahmen einer Online-Durchsuchung können jedoch unmittelbar andere Bereiche des infiltrierten Systems durchleuchtet werden, die nicht dem Kernbereichsschutz unterfallen. Ein sofortiger Abbruch der Durchsuchung bei Auffinden kernbereichsrelevanter Daten ist daher grundsätzlich nicht erforderlich. Daher genügt es, wenn sich der Kernbereichsschutz hier erst auf Beweisverwertungsebene und nicht bereits auf der Beweiserhebungsebene beachtet wird. Die Anforderungen an den Kernbereichsschutz sind auf der Erhebungsebene im Rahmen einer Online-Durchsuchung ein Stück weit zurückgenommen. Der Schutz vor Kernbereichsverletzungen zielt bei der Online-Durchsuchung nicht vordergründig darauf, das Festhalten eines nur flüchtigen, höchstvertraulichen Moments zu verhindern.[568] Stattdessen soll vermieden werden, dass aus einem Gesamtdatenbestand (von ohnehin digital vorliegenden Informationen) höchstvertrauliche Informationen ausgelesen werden, die jedoch in ihrer Gesamtheit regelmäßig nicht an die Vertraulichkeit des Verhaltens oder der Kommu-

566 Im Ergebnis auch Sinn, Stellungnahme zum Entwurf der BT-Drs. 18/11272, S. 12.
567 vgl. *Grözinger*, Die Überwachung von Cloud-Storage S. 309 ff.
568 BVerfGE 141, 220, Rn. 218 f.

nikation in einer Wohnung heranreichen.[569] Anders gestaltet sich dies jedoch im Falle einer Live-Überwachung. Die Situation einer Live-Überwachung ist identisch zu der einer Wohnraumüberwachung: Dem Betroffenen wird bei der Nutzung des informationstechnischen Systems in Echtzeit „über die Schulter geschaut"[570]. Sobald der Kernbereich betroffen ist, muss der Staat seine Live-Überwachung daher auch hier abbrechen. Da bezüglich der Live-Überwachung eine dem § 100d Abs. 4 S. 2 StPO entsprechende Regelung fehlt, hält *Grözinger* den Kernbereichsschutz des § 100d Abs. 4 S. 2 StPO für ungenügend.[571] Dem ist, sofern eine Live-Überwachung im Raum steht, zuzustimmen. Ob dies jedoch zur Verfassungswidrigkeit des § 100d StPO und damit auch zu einer Verfassungswidrigkeit des mit dem Kernbereichsschutz synallagmatisch verknüpften § 100b StPO führen muss, ist zweifelhaft. Es erscheint möglich, § 100d Abs. 3 StPO einer verfassungskonformen Auslegung zu unterziehen. Um dem verfassungsrechtlichen Interesse an einer Normerhaltung nachzukommen und zu verhindern, dass sich die gesetzgeberischen Kapazitäten in einer Fülle an Normkorrekturen erschöpfen, ist die verfassungskonforme Auslegung heute allgemein anerkannt.[572] Ihre Grenze findet sie jedoch dort, wo zum Wortlaut der Norm und zum gesetzgeberischen Willen ein ersichtlicher Widerspruch bestehen würde.[573] § 100d Abs. 3 S. 2 StPO enthält die Maßgabe, erlangte Informationen über den Kernbereich unverzüglich zu löschen. Solange es sich bei dem Zugriff nicht um eine Live-Überwachung handelt, stellt dies keinen Streitpunkt dar. Hinsichtlich der in Echtzeit durchgeführten Wohnraumüberwachung hat jedoch auch der Gesetzgeber erkannt und in § 100d Abs. 4 S. 2 StPO normiert, dass der Kernbereichsschutz hier besonders gefährdet erscheint. Bei Schaffung des § 100d Abs. 3 S. 2 StPO hatte der Gesetzgeber die Möglichkeit einer Online-Live-Durchsuchung in Form einer Online-Live-Überwachung und die offensichtliche Parallele zur Wohnraumüberwachung schlicht nicht vor Augen. Die Normierung des Gesamten § 100d StPO zeigt jedoch, dass der Kernbereichsschutz dem Gesetzgeber ein bedeutendes Anliegen war. Die hier vorgeschlagene Unterbrechung der Online-Überwachung in Echtzeit engt den Wortlaut des § 100d Abs. 3 S. 2 StPO auch nicht contra legem ein, sondern

569 BVerfGE 141, 220, Rn. 218 f.
570 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 5.
571 *Grözinger*, Die Überwachung von Cloud-Storage, S. 312.
572 *Voßkuhle*, AöR 2000, 177, 183; *Lüdemann*, Jus 2004, 27, 29; FS-Larenz/*Göldner*, 199, 200.
573 BVerfGE 110, 226, 267.

erweitert diesen im Sinne eines einheitlichen Schutzes des höchstpersönlichen Kernbereichs. § 100d Abs. 3 S. 3 StPO ist einer verfassungskonformen Auslegung zugänglich, die im Falle der live ablaufenden Online-Überwachung auch angezeigt erscheint. Eine Verfassungswidrigkeit der Vorschrift des § 100d Abs. 3 S. 2 StPO und damit auch des § 100b StPO ist nicht anzunehmen.

c) Zu weiter Anlasstatenkatalog

In der Entscheidung zum BKA-Gesetz wurden Eingriffe in das IT-Grundrecht nur zum Schutz überragend wichtiger Verfassungsgüter wie Leib, Leben, Freiheit der Person oder solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren, erlaubt.[574] Da der Straftatenkatalog des § 100b StPO als Anlasstaten jedoch auch solche Taten enthält, die keines der soeben genannten Rechtsgüter schützen (beispielsweise Geld- und Wertzeichenfälschung, § 100b Abs. 2 Nr. 1c StPO, der Hehlerei, § 100b Abs. 2 Nr. 1k StPO, der Geldwäsche, § 100b Abs. 2 Nr. 1 StPO oder der Bestechlichkeit und Bestechung, § 100b Abs. 2 Nr. 1m StPO), soll § 100b StPO verfassungswidrig sein.[575] Dabei wird jedoch verkannt, dass ebenso ein informationstechnisches System im Sinne des § 100b StPO betroffen sein könne, ohne den Eingriff am Maßstab des IT-Grundrechts messen zu müssen.[576] Wenn der Eingriff jedoch nur am Maßstab des Rechts auf informationelle Selbstbestimmung zu messen ist, können konsequenterweise auch Delikte, die keine überragend wichtigen Verfassungsgüter schützen, Anlass zu einer Online-Durchsuchung geben. Entscheidend ist also vielmehr, ob die gewonnenen Daten im konkreten Einzelfall einen derart tiefen Einblick in die persönliche Lebensgestaltung ermöglichen, dass ein Schutz durch das IT-Grundrecht erforderlich ist.[577] Dies wird bei einem privat genutzten informationstechnischen System anzunehmen sein, sodass in verfassungskonformer Auslegung des § 100b StPO eine Anordnung zur Online-Durchsuchung nur dann erfolgen darf, wenn der Tatverdacht hinsichtlich eines Delikts besteht, das dem Schutz eines der genannten wichtigen Rechtsgüter dient. Ebenso gut ist aber vorstell-

574 BVerfGE 120, 274, 326 f.
575 *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, S. 13.
576 BVerfGE 120, 274, 313.
577 BVerfGE 120, 274, 314.

bar, dass beispielsweise informationstechnische Systeme eines Unternehmens zur Nachverfolgung diverser Finanzströme infiltriert werden sollen. Im Zuge dessen wäre aber nicht zu erwarten ist, dass dadurch Inhalte offenbart werden, die das Erstellen eines umfassenden Persönlichkeitsprofils eines Menschen erlauben. In diesem Fall ist sodann auch nicht das IT-Grundrecht einschlägig, sondern lediglich das Recht auf informationelle Selbstbestimmung. Die Anordnung einer Online-Durchsuchung kann sodann in verfassungskonformer Weise auch aufgrund eines der „mindergewichtigen" Delikte aus dem Straftatenkatalog des § 100b StPO erfolgen. Somit ist § 100b StPO nicht aufgrund des normierten Straftatenkatalogs verfassungswidrig. Die Norm muss im Zuge ihrer Anwendung lediglich auch diesbezüglich im hier ausgeführten Umfang verfassungskonform angewandt werden.

d) Fehlerhafter Schutz von Berufsgeheimnisträgern

Zuletzt soll die Einschränkung in § 100d Abs. 5 S. 2 StPO, wonach sich der Schutz gegenüber Berufsgeheimnisträgern offenbarten Informationen aus § 100d Abs. 5 S. 1 StPO nicht auf deren Berufshelfer erstreckt, die Verfassungswidrigkeit der Vorschrift zum Kernbereichsschutz begründen.[578] § 100d Abs. 5 S. 1 StPO würde daher in solchen Fällen bedeutungslos, wenn auf den absolut geschützten Inhalt über einen Umweg rechtmäßig zugegriffen werden könnte. Gerade in der Praxis lässt sich organisatorisch kaum verhindern, dass bestimmte Kommunikation nicht höchstpersönlich mit dem Berufsgeheimnisträger, sondern auch mit dessen Berufshelfern, wie dem Sekretariat oder einer Arztgehilfin, erfolgt.[579] Jedoch gilt es zu beachten, dass § 100d Abs. 5 S. 2 StPO bezüglich gewonnener aber unter § 53a StPO fallender Erkenntnisse lediglich hinsichtlich der Frage der Verwertbarkeit eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes vorsieht. Eine Abwägung auf der Ebene der Beweiserhe-

578 Vgl. Stellungnahme des Deutschen Anwaltvereins zu dem Gesetzentwurf der Bundesregierung – Drs.18/11272, S. 11; abrufbar unter: https://anwaltverein.de/de/newsroom/sn-44-17-einfuehrung-der-online-durchsuchung-und-quellen-tkue?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2017/DAV-SN_44-17_%C3%84nderungsantrag.pdf (zuletzt abgerufen am 31.10.2021), S. 21; kritisch auch *Grözinger*, Die Überwachung von Cloud-Storage, S. 315; Az. der anhängigen Verfassungsbeschwerden: 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18.

579 *Basar/Hiéramente*, HRRS 2018, 336, 338.

bung ist gerade nicht vorgesehen. Insofern gewährleistet bereits § 100d Abs. 2 StPO die Unantastbarkeit des Kernbereichs privater Lebensgestaltung uneingeschränkt und losgelöst von jedweder Abwägung.[580] Zudem sind die gegenüber Berufshelfern getätigten Äußerungen auch auf der späteren Ebene der Beweisverwertung nicht uneingeschränkt, sondern nur unter Heranziehung eines Verhältnismäßigkeitskorrektivs verwertbar.

Aus der Rechtsprechung des Bundesverfassungsgerichts zu § 100c StPO ist zu folgern, dass Inhalte, die einem Gespräch mit einem Berufsgeheimnisträger entstammen, bereits auf Beweiserhebungsebene in der Regel einen höhere Schutzwürdigkeit aufweisen als solche mit bloßen Berufshelfern.[581] Dies ist auch angemessen, schließlich ist es nicht erforderlich, dass der Betroffene mit einem Berufshelfer in der gleichen Offenheit kommuniziert wie mit dem Berufsgeheimnisträger. Im Rahmen der ersten Kontaktaufnahme mit einer auf Strafrecht spezialisierten Kanzlei müssen beispielsweise gegenüber dem Sekretariat keine vertraulichen Details genannt werden, vielmehr wird der Hinweis auf ein laufendes Ermittlungsverfahren mit Angabe der entsprechenden vorgeworfenen Delikte genügen, um zu prüfen, ob ein persönlicher Termin zur Besprechung mit dem Rechtsanwalt in Frage kommt. Die Informationen über ein laufendes Ermittlungsverfahren stellt für die Strafverfolgungsbehörden jedoch keinen Mehrwert dar, sondern ist bereits bekannt.

Hinsichtlich einer Online-Durchsuchung ist die Differenzierung zwischen Berufgeheimnisträger und Berufshelfer zudem auch von untergeordneter Bedeutung. Denn es ist festzuhalten, dass das informationstechnische System in Form des Servers einer Kanzlei oder einer Praxis als Ganzes dem § 100d Abs. 5 S. 1 StPO unterfällt. Eine Differenzierung zwischen den informationstechnischen Systemen, die schwerpunktmäßig durch den Berufgeheimnisträger und solchen, die schwerpunktmäßig durch dessen Berufshelfer bedient werden, erscheint nicht rechtssicher durchführbar. Vielmehr stellt der Berufgeheimnisträger das komplette informationstechnische System zu Verfügung, weshalb es auch im Wege einer Gesamtbetrachtung einheitlich diesem zuzurechnen ist. § 100d Abs. 5 S. 2 StPO erlangt hinsichtlich der Online-Durchsuchung daher nur dann Bedeutung, wenn auf das private informationstechnische System der Berufshelfer zugegriffen werden soll. Dass ein Berufshelfer auf einem solchen in der Regel

580 BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR 543/06 -, Rn. 51 = teilweise in NJW 2007, 2753 ff.

581 BVerfG, Beschluss vom 15. Oktober 2009 – 2 BvR 2438/08 -, Rn. 12 = teilweise in NJW 2010, 287; BVerfGE 109, 279, 328.

keine Kanzleiinterna speichern sollte, ist daher ratsam. In einem solchen Fall müsste im Zuge einer Verhältnismäßigkeitsprüfung die Verwertbarkeit dieser Informationen geprüft werden. Von Bedeutung dabei könnte sein, ob der Rechtsanwalt den Informationen durch die Auslagerung eine geringe Vertraulichkeit beigemessen hat, was für eine Verwertbarkeit sprechen könnte. Auf der andern Seite könnte aber die Verwertung sogar den Schutzzweck des § 100d Abs. 5 S. 1 StPO umgehen, wenn dem Berufsgeheimnisträger die durch Art. 12 GG garantierte freie Wahl seiner Art der Berufsausübung (Arbeitsprozesse auf private informationstechnische Systeme seiner Angestellten auszuweiten) faktisch untersagt würde. Eine endgültige Abwägung kann stets nur im konkreten Fall vorgenommen werden.

e) Zwischenergebnis

Es erscheint daher gut vertretbar, wenn das BVerfG die bereits anhängige Verfassungsbeschwerde[582] hinsichtlich § 100b StPO zu Recht als unbegründet zurückweisen wird. § 100b StPO ist jedenfalls im Wege einer verfassungskonformen Auslegung verfassungsrechtlich nicht zu beanstanden.

5) Ergebnis

Hinsichtlich § 100b StPO ist zu konstatieren, dass Smart Speaker zwar hierunter zu subsumieren sind, der Erkenntnisgewinn in der Praxis jedoch begrenzt ist. Jedenfalls so lange eine Speicherung der Daten nicht auf der Hardware des infiltrierten Endgeräts erfolgt, können durch eine Infiltration dieses Gerätes keine ruhenden Daten abgegriffen werden. Hierfür wäre die Infiltration des Servers des Dienstleistungsanbieters erforderlich. Interessant bleibt einzig die Möglichkeit der Live-Überwachung im Rahmen des § 100b StPO. Insofern können Mikrofon und Kamera smarter Assistenten zwar nicht durch die Strafverfolgungsbehörden aktiviert werden, doch ist während einer aktiven Nutzung des Sprachassistenten das Mithören seitens der Strafverfolgungsbehörden möglich. Insofern stellen sich aber weitere Probleme im Rahmen der Verwertbarkeit der durch solch eine Live-Überwachung erlangten Informationen.

582 AZ: 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18.

VI) § 100c StPO

Eine weitere Möglichkeit Smart Speaker für die Strafverfolgung zu gewinnen, könnte die Durchführung einer Wohnraumüberwachung gem. § 100c StPO darstellen.[583] § 100c Abs. 1 StPO erhält die Befugnis, das von Personen „in einer Wohnung nichtöffentlich gesprochene Wort mit technischen Mitteln" abzuhören und aufzuzeichnen. Entsprechend gestattet die Vorschrift nach einhelliger Ansicht lediglich die akustische Überwachung und Aufzeichnung des nichtöffentlichen gesprochenen Wortes in Wohnungen.[584] Nicht ausdrücklich geregelt ist, ob die Wohnung zum Anbringen der für eine Überwachung erforderlichen Technik heimlich betreten werden darf. Insoweit ist aber, da der Inhalt der Norm ansonsten schlicht nicht umsetzbar wäre, von einer Annexkompetenz auszugehen.[585] In eben dieser Verwanzung eines Wohnraums liegt allerdings ein nicht zu unterschätzendes praktisches Problem. Die Strafverfolgungsbehörden dürfen, während sie die Räume, in welchen sich der Beschuldigte mutmaßlich aufhält, präparieren, nicht entdeckt werden, da ansonsten die Heimlichkeit und damit der Erfolg der Maßnahme in Gefahr gerät. Vielmehr bestünde dann die Gefahr, dass der Betroffene den Umstand, dass seine Wohnung verwanzt ist für sich ausnutzt und den Strafverfolgungsbehörden, die von einer heimlichen Überwachung ausgehen, gezielt falsche Informationen zukommen lässt. Da für das Verwanzen einer Wohnung mitsamt dem Anbringen der notwendigen Technik zuweilen mehrere Stunden einzuplanen sind, stellt dies ein erhebliches Risiko dar. Der Betroffene darf nicht vor dem Ende der Verwanzung in seine Wohnung zurückkehren.[586] Hinzu kommt die Gefahr, dass verbaute Wanzen durch die Betroffenen entdeckt werden und sodann die Verbindung getrennt wird. Neben der aufzuwendenden Zeit wurden auch wegen der für eine Wohnraumüberwachung anfallenden Kosten kritisiert, dass „Aufwand und Ertrag in keinem Verhältnis zueinander stünden"[587]. In den vergangenen Jahren sank

583 Als theoretische Idee jedoch im Rahmen des § 100b StPO bereits bei *Kruse/Grzesiek*, KritV 2017, 331, 335.

584 *Günther* in: MüKo-StPO, § 100c StPO, Rn. 3; *Bruns* in: KK-StPO, § 100c StPO, Rn. 4.

585 *Bruns* in: KK-StPO, § 100c StPO, Rn. 4; *Hegmann* in: BeckOK-StPO, § 100c StPO, Rn. 3.

586 *Meyer-Wieck*, Der große Lauschangriff, S. 136.

587 *Wolter* in: SK-StPO, § 100c StPO, Rn. 10a; *Hauck* in: LR-StPO, § 100c StPO, Rn. 5.

die Zahl angeordneter Wohnraumüberwachungen unter anderem daher auf durchschnittlich sieben Anordnungen pro Jahr.[588]

Diese Probleme könnten vermieden werden, wenn sich die Strafverfolgungsbehörden die Mikrofone eines Gegenstandes, den der Betroffene selbst in seine Wohnräume verbringt, als Wanze zu Nutzen machen dürften. Insofern könnte das Mikrofon des Endgerätes genutzt werden, um Gespräche aus der Wohnung mitzuhören und aufzuzeichnen.

1) Smart Speaker als technisches Mittel im Sinne des § 100c StPO

Hierzu müsste es sich bei dem Endgerät, welches als Wanze dienen soll, um ein technisches Mittel im Sinne des § 100c StPO handeln. Hierunter werden die klassischen Abhöreinrichtungen wie batteriebetriebene Minisender (sog. Wanzen), modernere GSM-Abhörgeräte oder Richtmikrofone gefasst. Die Akkulaufzeit solcher Wanzen beträgt jedoch in der Regel zwischen fünf Stunden bis maximal vier Tagen. GSM-Abhörgeräte verfügen zwar über deutlich größere Laufleistung, sind aufgrund ihrer Größe jedoch auch schwerer zu verstecken.[589] Neben dem Installationsaufwand könnten auch solche praktischen Probleme durch Nutzung der Mikrofone des Endgeräts eines Sprachassistenten umgangen werden.

a) Wortlaut

Nach dem Wortlaut lässt sich der Geltungsbereich der Vorschrift nicht exakt eingrenzen. Schließlich handelt es sich bereits immer dann um ein Mittel, wenn die Nutzung einer Sache der Erreichung eines bestimmten Zieles dienlich ist.[590] Das technische Endgerät würde zur Wohnraumüberwachung eingesetzt und es ermöglichen das in der Wohnung Gesprochene wahrzunehmen und aufzuzeichnen. Der Wortlaut der Norm lässt keine Zweifel aufkommen, dass es sich dann bei einem solchen Endgerät um ein technisches Mittel im Sinne des § 100c StPO handelt.

---

588 *Wolter* in: SK-StPO, § 100e StPO, Rn. 6.
589 *Hauck* in: LR-StPO, § 100c StPO, Rn. 85.
590 Duden, Bedeutung des Wortes „Mittel“, abrufbar unter: https://www.duden.de/rechtschreibung/Mittel_Arznei_Geld_Behelf (zuletzt abgerufen am 31.10.2021).

b) Historie

Gemessen an einer historischen Betrachtung des § 100c StPO könnte zu fordern sein, dass es sich bei technischen Mittel im Sinne des § 100c StPO um solche der Strafverfolgungsbehörden handeln müsse, da andernfalls die diesen zustehende Annexkompetenz, die Wohnung des Beschuldigten für Installationszwecke zu betreten, obsolet wäre.[591] Eine solche Annexkompetenz würde es schließlich nur dann benötigen, wenn im Eigentum des Staates stehende technische Geräte in die Wohnung verbracht und dort angeschlossen werden müssen. Naheliegender ist mit Blick auf die angezeigte Annexkompetenz, jedoch der Schluss, dass mit diesem Zugeständnis keineswegs die Annahme einhergehen sollte, dass die Strafverfolgungsbehörden eigene Mittel einzusetzen haben. Vielmehr sollte allein für den Fall, dass ein solches Anbringen in der Wohnung notwendig würde das hierzu erforderliche Betreten miterfasst sein. Dass der Gesetzgeber mit dem Zuerkennen dieser Annexkompetenz zum Ausdruck bringen wollte, dass die Strafverfolgungsbehörden eigene technischer Mittel einzusetzen haben, ist den Gesetzesbegründungen nicht zu entnehmen. Im Hinblick auf die zeitliche Entstehung der Norm kann dies auch nicht weiter verwundern.[592] In den zurückliegenden Jahrzehnten war schlicht noch nicht denkbar, dass eines Tages auch nicht der Strafverfolgungsbehörde gehörende technische Mittel zu einer Wohnraumüberwachung genutzt werden könnten.

c) Systematik

Gegen die Heranziehung des Endgeräts des Betroffenen soll ferner eine systematische Auslegung unter verfassungsrechtlichen Gesichtspunkten sprechen. Die Pflicht zur Nutzung staatlicher Mittel für eine Maßnahme gem. § 100c StPO wird laut *Rüscher* im Rahmen einer systematischen Betrachtung deutlich. Bei Betrachtung der Ermittlungsmaßnahmen in den §§ 94 bis 111q StPO wird der Begriff des technischen Mittels in diversen Normen genannt (§§ 100a, 100b, 100c, 100f, 100h, 100i StPO). Dabei handle es sich allerdings stets um eigene Mittel der Straf-

591 *Rüscher*, NStZ 2018, 687, 690; *Brodowski* in: BeckOK-ITR, X, § 100c StPO, Rn. 6.

592 Die Regelung des § 100c StPO trat durch das Gesetzes zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 04.05.1998 in Kraft, vgl. BT-Drs. 13/8651, S. 10.

verfolgungsbehörden. Dies würde vor allem anhand der §§ 100a Abs. 1 S. 2, 100b Abs. 1 StPO deutlich, da dort mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen werde.[593] Daher sei das informationstechnische System dem Betroffenen zuzuordnen, während das technische Mittel der Strafverfolgungsbehörde zugeordnet sein müsse.[594] Bereits diese Maßstabsbildung erscheint jedoch angesichts des weiten Wortlauts nicht überzeugend.[595] Selbst wenn man jedoch diesen Maßstab zugrunde legen würde, so wäre die aufgespielte Software zur Aktivierung des Mikrofons als das staatliche Mittel zu sehen. Dagegen kann nicht vorgebracht werden, dass es alleine durch das technische Mittel der Software nicht möglich wäre, das in einer Wohnung gesprochene Wort aufzuzeichnen, sondern das entscheidende technische Mittel das informationstechnische Systems des Betroffenen sei, welches für das Aufzeichnen der Gespräche unabdingbar ist.[596] Denn im Unterschied zu § 100b StPO fordert der Wortlaut des § 100c StPO gerade kein dem Betroffenen zuzuordnendes informationstechnisches System, sondern setzt lediglich das Abhören mittels eines technischen Mittels voraus.

Hinzu kommt, dass auch ein Vergleich mit § 100i StPO kein anderes Ergebnis nahe legt. Gem. § 100i Abs. 1 Nr. 2 StPO darf durch technische Mittel der Standort eines Mobilfunkendgerätes ermittelt werden. Das technische Mittel stellt hierbei der sog. IMSI-Catcher dar, durch den eine virtuelle Funkzelle aufgebaut wird, in die sich das Mobiltelefon des Betroffenen irrtümlich einwählt.[597] Obiger Argumentation folgend, müsste aber konstatiert werden, dass das entscheidende Mittel zur Standortbestimmung das Mobiltelefon des Betroffenen darstellt. Ohne dieses wäre eine Standortbestimmung nicht möglich. Dadurch wird deutlich, dass es gerade nicht ausgeschlossen ist, dass die Strafverfolgungsbehörden durch ein eigenes technisches Mittels wiederum ein technisches Mittel des Betroffenen im Sinne der Strafverfolgung „manipulieren". Die aufgespielte Software auf das Endgerät des Betroffenen kann daher mit dem IMSI-Catcher, der Smart Speaker im Eigentum des Betroffenen mit dessen Mobiltelefon im Rahmen des § 100i StPO verglichen werden. Aus dem Kanon der Eingriffs-

593 *Rüscher*, NStZ 2018, 687, 690.
594 *Rüscher*, NStZ 2018, 687, 690; *Weber*, jM 2021, 252, 256; *Brodowski* in: BeckOK-ITR, X, § 100c StPO, Rn. 7; ablehnend *Anders*, ZJS 2020, 70, 77.
595 zutreffend auch *Anders*, ZIS 2020, 70, 77.
596 *Rüscher*, NStZ 2018, 687, 690.
597 BVerfG, Beschluss vom 22. August 2006 – 2 BvR 1345/03, Rn. 14.

befugnisse ergibt sich daher nicht zwangsläufig, dass das entscheidende technische Mittel dem Staat zuzuordnen sein muss.

d) Telos

Sinn und Zweck der 1998 geschaffenen Wohnraumüberwachung war es, den bis dahin von heimlichen staatlichen Ermittlungen ausgenommen Wohnraum abhören zu können.[598] Der Gesetzgeber hatte im Rahmen der Ausgestaltung der Norm jedoch darauf verzichtet, konkrete Mittel zu benennen, um den Strafverfolgungsbehörden zu ermöglichen, entsprechend der technologischen Entwicklung auf diejenige Technik zurückgreifen zu können, die für die konkrete Maßnahme am geeignetsten erscheint.[599] Von dieser Entwicklung umfasst ist aber nicht nur die technische Fortentwicklung von Richtmikrofonen bis hin zur Möglichkeit über eine Laserabtastung Schallwellen an Fenstern abzufangen und in gesprochene Worte rückzuübersetzen,[600] sondern auch solche technische Geräte für Abhörmaßnahmen zu nutzen, die Betroffene freiwillig in ihrer Wohnung verwahren. Sinn und Zweck der Vorschrift ist einzig aus der Ferne einen Zugriff auf in diesem Moment gesprochene Worte zu ermöglichen. Aus teleologischen Gesichtspunkten spricht daher nichts gegen die Annahme, das Endgerät des Betroffenen mittels einer Software zur staatlichen Wanze umzuwandeln. Das eine solche Möglichkeit der Strafverfolgungsbehörden existiert, erkannte das BVerfG bereits im Jahr 2008 als es formulierte, dass mittels der Infiltration eines informationstechnischen Systems zur Nutzung der an das System angeschlossenen Peripheriegeräte (bspw. ein Mikrofon), bestimmte Vorgänge innerhalb der Wohnung überwacht werden könnten.[601]

2) Kollision mit IT-Grundrecht

Das Aufspielen einer Software zur permanenten akustischen Überwachung soll einen Eingriff in das aus Art. 2 Abs. 1 GG i.V.m. Art 1 Abs. 1 GG abgeleitete Grundrecht der Integrität informationstechnischer Systeme be-

598 BGBl. I 845; *Günther* in: MüKo-StPO, § 100c StPO, Rn. 1.
599 *Günther* in: MüKo-StPO, § 100c StPO, Rn. 50.
600 *Hauck* in: LR-StPO, § 100c StPO, Rn. 85.
601 BVerfGE 120, 274, 310.

gründen. Die damit verbundene Eingriffsintensität ginge jedoch über das hinaus, was der Gesetzgeber bei Erlass des § 100c StPO intendierte, da der Gesetzgeber sich über einen solchen Grundrechtseingriff in das IT-Grundrecht bei Erlass des § 100c StPO nicht bewusst war.[602]

Bewusst musste sich der Gesetzgeber jedoch sein, dass mit jeder Abhörmaßnahme jedenfalls ein Eingriff in das aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG entspringende Recht auf informationelle Selbstbestimmung einhergeht.[603] Denn das Recht auf informationelle Selbstbestimmung schützt vor jeder Form der Erhebung, schlichter Kenntnisnahme oder auch Speicherung von persönlichen Informationen.[604] Damit kann aus diesem Recht auch das Recht Herr über das eigene gesprochene Wort zu bleiben, also frei darüber bestimmen zu können, welchen Personen Zugang zum eigenen gesprochenen Wort gewährt werden soll, abgeleitet werden. Jenes im Privaten gesprochene Wort wollen sich die Strafverfolgungsbehörden im Rahmen des § 100c StPO jedoch zu eigen machen. Mit dem Abhören des gesprochenen Wortes über das Endgerät geht daher zwar ein Eingriff in das Recht auf informationelle Selbstbestimmung, nicht jedoch ein Eingriff in das Grundrecht der Integrität informationstechnischer Systeme einher. Dieses Grundrecht soll seinen Inhaber vor einem unberechtigten Zugriff auf die auf einem informationstechnischen System gespeicherten Daten schützen. Sofern die Strafverfolgungsbehörden allerdings das Endgerät bildlich gesprochen zur Wanze umfunktionieren, soll gerade kein Zugriff auf gespeicherte Datenbestände erfolgen, sondern das aktuell gesprochene Wort unter den strengen Voraussetzungen des § 100c StPO abgehört werden. Letztlich handelt es sich dabei um das Ergebnis mitsamt der gleichen Eingriffsintensität, das auch durch das Anbringen von Wanzen oder anderen Abhörinstrumenten in der Wohnung des Beschuldigten eintreten würde. Ein zusätzlicher Schutz durch das IT-Grundrecht erscheint daher für die hier zugrunde liegende Sachverhaltskonstellation weder erforderlich, noch liegen die Voraussetzungen für die Eröffnung dessen Schutzbereiches vor. Als problematisch erweist sich jedoch, dass auch wenn durch das Aufspielen der Überwachungssoftware zum kontrollierten Einsatz des Mikrofons der Schutzbereich des IT-Grundrecht nicht eröffnet ist, ein Zugriff auf ein informationstechnisches System im Sinne der Strafprozessordnung vorliegen könnte. Ein solcher Zugriff

602 *Rüscher*, NStZ 2018, 687, 690; *Marx*, DVBl 2020, 488, 492 bzgl. § 46 Abs. 1 BkAG.
603 BVerfGE 109, 279, 365.
604 *Di Fabio* in: Maunz/Dürig-GG, Art. 2 Abs. 1 GG, Rn. 176.

auf ein informationstechnisches System sollte nach dem Willen des Gesetzgebers nur unter den Voraussetzungen des § 100b StPO erfolgen.[605] In der Literatur wird daher vereinzelt vermutet, dass der Zugriff auf ein informationstechnisches System zur Softwareinstallation zwecks der Durchführung eines Lauschangriff mittels eines Smart Home Endgeräts eher bei § 100b StPO zu verorten sein dürfte.[606]

3) Stellungnahme

Der Wortlaut und auch eine historische Betrachtung lassen nicht daran zweifeln, „Smart Home" Endgeräte als Ohr der Strafverfolgungsbehörden im Rahmen des § 100c StPO nutzen zu können. Den Zweck einer solchen heimlichen Aufzeichnung betrachtend, erscheint es ebenfalls möglich dies auf dem Wege zu erreichen, ein technisches Gerät des Betroffenen als Abhörquelle zu nutzen. Lediglich die systematische Sichtweise erhebt gegen die Umwandlung des Endgeräts zur Wanze Bedenken. Der zum Abhören erforderliche Zwischenschritt bedarf das Aufspielen einer Software und daher jedenfalls ein Zugriff auf die Software des informationstechnischen Systems des Endgeräts. Es bleibt zu fragen, ob der Zugriff auf ein solches System nur unter Heranziehung des § 100b StPO möglich ist. Dies mag auf den ersten Blick nahe liegen, nennt doch lediglich der Wortlaut des § 100b StPO die Befugnis zum Eingriff in ein informationstechnisches System. Jedoch greift eine solche Betrachtung zu kurz. § 100b StPO regelt den Eingriff in ein informationstechnisches System, um aus diesem Daten zu erheben. Im Rahmen des Lauschangriffs unter Nutzung des sich in der Wohnung befindlichen Smart Speakers sollen aus dem informationstechnischen System jedoch gerade keine Daten erhoben werden, sondern vielmehr in der Wohnung ablaufende Vorgänge überwacht werden. Sämtliche auf dem System gespeicherten Informationen über den Nutzer bleiben unberührt. Obwohl zur Zielerreichung auf ein informationstechnisches System zugegriffen wird, ist aufgrund der vollkommen unterschiedlichen Zielrichtung einer Wohnraumüberwachung im Vergleich zu einer Online-Durchsuchung kein systematischer Konflikt zwischen den Befugnisnormen des § 100b StPO und § 100c StPO auszuma-

605 BS-Drs. 19/11478 als Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Stephan Thomae, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP, S. 3.

606 *Blechschmitt*, MMR 2018, 361, 365.

chen. Während bei der Online-Durchsuchung das informationstechnische System selbst nach Informationen durchsucht wird, soll bei der Wohnraumüberwachung lediglich das informationstechnische System als Wanze dienen. Diese Sichtweise steht daher auch in keinem Widerspruch zu der einhelligen Auffassung, dass § 100c StPO selbstredend keine Befugnis für eine Online-Durchsuchung enthält.[607] Denn zu einer solchen Online-Durchsuchung kommt es im hier genannten Fall gerade nicht. Ferner ist festzuhalten, dass die hohe Eingriffsintensität eines Vorgehens nach § 100b StPO nicht bereits durch die bloße technische Infiltration eines informationstechnischen Systems begründet wird. Denn allein dadurch wäre es nicht möglich persönlichkeitsrelevante Daten über den Betroffenen zu erhalten. Vielmehr bedarf es hierfür eines zweiten Schrittes, die durch die Infiltration geschaffene Möglichkeit, das System nach Informationen zu durchsuchen, sodann auch aktiv auszunutzen. Da es bei der Infiltration des Smart Speakers zur Nutzung des Mikrofons nicht zu diesem zweiten Schritt einer aktiven Durchsuchung kommt, liegt auch kein Eingriff in das IT-Grundrecht vor. Dieses schützt nicht bereits die Unantastbarkeit technischer Systeme an sich, sondern kommt erst im Zusammenspiel mit der Gefahr einer aus diesem System erfolgten Informationsgewinnung zum Tragen.[608] Insofern führt auch das BVerfG aus, dass das IT-Grundrecht beim Zugriff auf informationstechnische Systeme anzuwenden sei, wenn dieses System Daten des Betroffenen in einem derartigen Umfang enthält, dass durch den Zugriff auf das System ein Einblick in wesentliche Teile der Lebensgestaltung einer Person gegeben wäre oder ein aussagekräftiges Bild der Persönlichkeit daraus abzuleiten wäre.[609] Das Gericht hält das IT-Grundrecht folglich nur dann für das einschlägige Grundrecht, wenn das informationstechnische System die entsprechende Datenvielfalt in sich enthält. Im Rahmen der Wohnraumüberwachung stellt allerdings keineswegs der Zugriff auf die in dem als Wanze genutzten System möglicherweise enthaltenen Daten das Ziel der Strafverfolgungsbehörden dar. Vielmehr sollen mittels des informationstechnischen Systems neue – von dem informationstechnischen System als solchem unabhängige – Gespräche in der Wohnung abgehört werden. Die entsprechenden Daten sind folglich

607 *Eschelbach* in: SSW-StPO, § 100c StPO, Rn. 5.

608 A.A. *Hoffmann-Riem*, JZ 2008, S. 1009, 1019, der den Schutz des IT-Grundrechts auf sämtliche infolge einer Infiltration gewonnen Informationen erstreckt; *Meinicke*, DSRITB 2018, 835, 851, der einen Eingriff in das IT-Grundrecht bei jedweder Infiltration eines informationstechnischen Systems für angezeigt erachtet; *Marx*, DVBl 2020, 488, 492.

609 BVerfGE 120, 274, 314.

nicht im infiltrierten Gerät enthalten, sondern werden erst durch dessen Nutzung als Wanze erschaffen.

Ferner kommt dem IT-Grundrecht nach der Rechtsprechung des BVerfG nur dann Bedeutung zu, wenn durch einen Zugriff auf ein informationstechnisches System auch Daten erhoben werden, die wiederum nicht durch die übrigen Grundrechte vor einem Zugriff geschützt sind.[610] Nur in diesem Fall bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner im IT-Grundrecht erlangten Ausprägung zu schließen ist.[611] Das Bundesverfassungsgericht ist demnach der Ansicht, dass nur, sofern kein Schutz durch die Grundrechte der Art. 10 GG, Art. 13 GG oder durch das Recht auf informationelle Selbstbestimmung gewährleistet werden kann, die Infiltration eines informationstechnischen Systems auch eine Beeinträchtigung darstellt, die den Schutz durch das IT-Grundrechts bedarf.[612] Dies bedeutet aber gleichfalls, dass es das Bundesverfassungsgericht für möglich erachtet, dass durchaus ein informationstechnisches System infiltriert werden kann und dennoch ein ausreichender Schutz durch die genannten Grundrechte besteht. Mithin, dass nicht jede Infiltration eines solchen Systems den Schutz des neu geschaffenen IT-Grundrechts bedarf. Insofern ist zudem zu beachten, dass das BVerfG in seiner Entscheidung zur Online-Durchsuchung einen Schutz durch das IT-Grundrecht nur deshalb für notwendig erachtete, da die lediglich auf dem heimischen Rechner ruhenden Daten nicht in den Schutzbereich des Art. 10 GG fielen und ansonsten eine Schutzlücke bestanden hätte.[613] Hätte daher in der gleichen Situation ein Schutz durch andere Grundrechte bestanden, so hätte das Gericht trotz der vorhanden Infiltration des Systems kein Schutz durch das IT-Grundrecht für notwendig erachtet.

Bei der Infiltration eines Endgeräts zur Nutzung des Mikrofons schützen jedoch unter Umständen bereits das Grundrecht aus Art. 13 GG sowie in jedem Falle das aus dem Recht der informationellen Selbstbestimmung abgeleitete Recht am eigenen gesprochenen Wort den Betroffenen hinreichend.[614] Im Urteil zur Online-Durchsuchung stellte auch das Bundesverfassungsgericht fest, dass es unter anderem dem Schutzbereich des Art. 13 GG unterfiele, wenn mittels der Infiltration eines sich einer Woh-

610 BVerfGE 120, 274, 308.
611 BVerfGE 120, 274, 308.
612 BVerfGE 120, 274, 302; *Gercke* in: HK-StPO, § 100b StPO, Rn. 2.
613 BVerfGE 120, 274, 307 f.; vgl. auch *Gähler*, HRRS 2016, 340, 345.
614 Vgl. bzgl. der Legitimation mittels § 100c StPO einen Eingriff in diese Grundrechte zu rechtfertigen, *Gercke* in: HK-StPO, § 100c StPO, Rn. 1.

nung befindlichen informationstechnischen Systems, bestimmte Vorgänge innerhalb einer Wohnung mittels der an dem System angeschlossenen Mikrofone überwacht werden sollen.[615] Zwar würde Art. 13 GG keinen Schutz gegen die infolge der Infiltration mögliche Datenerhebung aus dem System bieten,[616] doch ist dies im hiesigen Kontext aus zwei Gründen nicht von Bedeutung. Zum einen soll es wie dargelegt zu einer solchen Datenerhebung aus dem System gar nicht kommen. Zum anderen sind auf dem infiltrierten Endgerät in Form eines Smart Speakers im Unterschied zu einem Personalcomputer auch keine Datenbestände gespeichert, sodass eine solche Erhebung bereits aus praktischen Gesichtspunkten ausscheidet und eine Kollision mit dem IT-Grundrecht nicht zu befürchten ist.[617] Somit handelt es sich bei der Manipulation eines Smart Speakers nicht um einen Zugriff in ein informationstechnisches System, durch den auf dem System vorhandene Daten ganz oder teilweise ausgespäht werden sollen oder können. Es besteht mithin auch nicht die Gefahr, durch eine Datenerhebung *aus* dem informationstechnischen System „*einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten*“[618]. Im Übrigen erscheint es widersprüchlich, das insofern mildere Vorgehen eines ferngesteuerten Softwarezugriffs zu versagen, jedoch zu erlauben, die Wohnung des Betroffenen durch mehrere Beamte zu betreten und sodann im Smart Speaker eine zusätzliche Hardwarekomponente oder eine Wanze zu verbauen. Ferner ist zu beachten, dass die Anordnung der Wohnraumüberwachung hohen Hürden unterliegt, sodass nicht die Gefahr besteht, dass jeder Nutzer eines Smart Speakers infolge der einfacheren Möglichkeit der Strafverfolgungsbehörden eine Wohnraumüberwachung ohne aufwendige Verkabelung der Wohnung durchführen zu können, vorschnell Betroffener einer solchen Maßnahme zu werden droht. Nach alledem ist der Zugriff auf Smart Speaker zur Durchführung eines Lauschangriffs unter den Voraussetzungen des § 100c StPO zuzulassen.[619] Durch § 100c StPO nicht gedeckt bleibt der Zugriff auf das Endgerät, um dessen Kamera für eine visuelle

615 BVerfGE 120, 274, 310.
616 BVerfGE 120, 274, 311.
617 Anders könnte dies zu beurteilen sein, wenn ein Sprachassistent in einem Smartphone integriert ist, auf welchem selbst wiederum persönlichkeitsrelevante Daten gespeichert sind.
618 BVerfGE 120, 274, 314.
619 Offenlassend *Gless*, StV 2018, 671, 674; *Anders,* ZIS 2020, 70, 76; ablehnend *Rüscher*, NStZ 2018, 687, 690; *Meinicke*, DSRITB 2018, 835, 851; *Weber,* jM 2021, 252, 256; *Brodowski* in: BeckOK-ITR, X, § 100c StPO, Rn. 6 f.

Überwachung zu nutzen. Art. 13 Abs. 3 GG sowie § 100c StPO umfassen nach ihrem ausdrücklichen Wortlaut lediglich die akustische nicht aber die visuelle Wohnraumüberwachung.

4) Verpflichtung der Hersteller zur Mitwirkung

Darüber hinaus stellt sich die Frage, ob die Strafverfolgungsbehörden die Hersteller smarter Endgeräte verpflichten können, in ihre Geräte „Hintertüren" (sog. backdoors) einzubauen, um das Mikrofon ohne gesonderten Hack der Behörden zu aktivieren.[620] Bereits der ehemalige Bundesinnenminister de Maizière, forderte Hintertüren in IT-Systemen, damit Lausch- und Überwachungsbefugnisse nicht durch technische Sicherungen erschwert werden.[621] Hierzu müssten die Systeme bereits bei ihrer Anfertigung mit entsprechenden Funktionen oder Sicherheitslücken ausgestattet werden.[622] Damit ginge jedoch einher, dass solche bewusst geschaffenen Sicherheitslücken auch von Dritten unberechtigten Personen genutzt werden könnten. Die Anbieter zu verpflichten, die bestehende Sicherungen gezielt auszulassen ist daher mit den seit 20 Jahren geltenden Krypto-Eckpunkten der Bundesregierung nicht zu vereinbaren.[623] Kryptografische Backdoors würden eine enorme Gefahr gegenüber der organisierten Kriminalität, Akteure der Wirtschaftsspionage oder ausländische Geheimdiensten begründen.[624] Eine entsprechende Ermächtigungsgrundlage zum Einbau solcher Hintertüren kann damit nicht verfassungskonform sein.[625] Zwar stellt das Nachverfolgen konkreter Verdachtslagen ein legitimes staatliches Sicherheitsinteressen dar, sodass auch unterschiedlich geartete Zugriffe auf technologische Endgeräte möglich sein müssen. Auch wenn durch die Existenz von Kryptografie dieser Zugriff unweigerlich wesentlich erschwert wird, kann die Schwächung dieser Errungenschaft der Kryptopolitik aus den späten 90er Jahren jedoch keine verfassungsrechtlich verhältnismäßige Gangart zur Erreichung einer einfacheren Strafverfolgung sein.[626] Die generelle Absenkung des Sicherheitsstandards un-

620 *Krempl*, c´t 2019, Heft 14, 36.
621 Vgl. *Schaar*, MMR 2018, 125, 126; *Blechschmitt*, MMR 2018, 361, 365 m.w.N.
622 *Derin/Golla*, NJW 2019, 1111, 1112.
623 MMR 1999, XVII, XVIII; *Krempl*, c´t 2019, Heft 14, 36; vgl. auch § 4, B.), V), 1) a).
624 *Hornung*, MMR 2015, 145, 146.
625 *Hornung*, MMR 2015, 145, 146; *Meinicke*, DSRITB 2012, 773, 776.
626 *Hornung*, MMR 2015, 145, 146.

terschiedlicher Technologien würde ein Einfallstor für Kriminelle unterschiedlichster Richtungen darstellen und kann mit dem einfacheren und weniger komplizierten Zugriff auf entsprechende Systeme nicht aufgewogen werden. Gerade angesichts der großen Menge an dadurch weniger geschützten unbeteiligten IT-Systemen und den im Vergleich hierzu verschwindend geringen Zugriffen der Strafverfolgungsbehörden auf solche Systeme kann ein angemessener Interessensausgleich nicht hergestellt werden.

VII) Kombination aus § 100b und § 100c StPO

Sofern die Durchführung des Lauschangriffs unter Heranziehung des § 100c StPO abgelehnt wird, wird angedacht diesen durch ein Zusammenspiel der §§ 100b, 100c StPO zu legitimieren. Nur auf diesem Wege könnte unter Heranziehung des § 100b StPO in ein informationstechnisches System eingegriffen werden, um unter Heranziehung des § 100c StPO gleichfalls in Art. 13 GG einzugreifen.[627] Zwar sprechen keine Gründe gegen den gleichzeitigen Einsatz mehrerer heimlicher Ermittlungsmethoden, sofern diese dem Grundsatz der Verhältnismäßigkeit entsprechen und daher nicht zu einer Rundumüberwachung mitsamt einer umfassenden Erstellung eines Persönlichkeitsprofils führen.[628] Dennoch wurde der durch *Rüscher* vorgebrachte Gedanke durch diesen sogleich wieder verworfen. In der Kombination der §§ 100b, 100c StPO würde kein gleichzeitiger Einsatz der Ermittlungsbefugnisse im Sinne einer parallel ablaufenden Online-Durchsuchung und einer zeitgleich ablaufenden Wohnraumüberwachung stattfinden, sondern es würde eine einheitliche Überwachungsmethode aus zwei getrennt voneinander zu betrachtenden Ermittlungsbefugnissen als „neuartiges Ermittlungsmittel" geschaffen.[629] Unabhängig davon, dass es eines solchen Konstrukts, aufgrund der bestehenden Zugriffsmöglichkeit nach § 100c StPO, nicht bedarf, würde aufgrund der Frage welche Eingriffsvoraussetzungen einem solchen Zusammenspiel aus bestehenden Ermächtigungsgrundlagen zu Grunde zu legen wären, eine gewisse Rechtsunsicherheit entstehen, die weder erforderlich ist und die es im Übrigen auch generell zu vermeiden gilt.

---

627 *Rüscher*, NStZ 2018, 687, 692.
628 BVerfGE 112, 304, 319.
629 *Rüscher*, NStZ 2018, 687, 692.

VIII) § 100f StPO

Neben der Möglichkeit im Rahmen des „großen Lauschangriffs" auf Smart Speaker in Wohnungen zuzugreifen, bleibt die Frage, ob daneben auch außerhalb von Wohnungen – beispielsweise auf die in Smartphones verbauten Sprachassistenten – zugegriffen werden kann. Dies wäre vor allen Dingen von großem Interesse, wenn die Verdächtigen während eines Spaziergangs oder – gerade bei Delikten des Wirtschaftsstrafrechts – im Büro abgehört werden sollen. Seinem Wortlaut nach erlaubt § 100f StPO das Abhören oder Aufzeichnen des außerhalb von Wohnungen gesprochenen nichtöffentlichen Wortes mit technischen Mitteln. Als Eingriffsvoraussetzung erfordert er zudem lediglich das Vorliegen einer Katalogtat nach § 100a Abs. 2 StPO anstelle wie § 100c StPO das Vorliegen einer in § 100b Abs. 2 StPO genannten Tat. Im Unterschied zu § 100c Abs. 1 Nr. 4 StPO ist darüber hinaus lediglich gefordert, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise mindestens wesentlich erschwert aber nicht unverhältnismäßig erschwert wäre. Im Übrigen sind die Eingriffsvoraussetzungen bis auf § 100c Abs. 1 Nr. 3 StPO gleich. Die im Gesamten milderen Eingriffsvoraussetzungen bei § 100f StPO legen daher bereits aufgrund eines Erst-Recht-Schlusses nahe, dass die Strafverfolgungsbehörden, wenn schon die Überwachung gar in der besonders schützenswerten Wohnung des Betroffenen erlaubt ist, erst Recht außerhalb der Wohnung von diesem geführte Konversationen abhören können. Hinsichtlich der Voraussetzung, dass dieser Zugriff mittels eines technischen Mittels erfolgen muss, kann im Vergleich zu § 100c StPO nichts anderes gelten.[630]

IX) §§ 102 ff., 110 Abs. 3 StPO

Die dargestellten heimlichen Überwachungsmöglichkeiten werden ergänzt durch die der offenen Ermittlungsbefugnisse. Zentraler Bestandteil hiervon sind die Durchsuchungsvorschriften der §§ 102 ff. StPO. Ziel einer solchen Durchsuchung ist entweder die Ergreifung des Verdächtigen (Ergreifungsdurchsuchung) oder das Auffinden von Beweismitteln (Ermittlungsdurchsuchung). Die §§ 102, 103 StPO ermächtigen jedoch zum einen lediglich zu einer groben Sichtung durch Inaugenscheinnahme.[631] Zum

630 Vgl. oben A. VI).
631 *Süptitz/Utz/Eymann*, DuD 2013, 307, 308.

anderen enthalten sie auch keine Reglung auf elektronisch archivierte Datenbestände zuzugreifen, die sich nicht in den Räumlichkeiten des Durchsuchungsobjekts befinden, da sie dezentral in einer Cloud gespeichert sind.[632] Die detailliertere Durchsicht von aufgefundenen Papieren oder ganzen Aktenordnern wird in § 110 StPO gesondert geregelt ist. Bezüglich elektronisch gespeicherter Daten von besonderer Relevanz ist dabei § 110 Abs. 3 StPO, der auch die Durchsicht extern abgelegter elektronischer Daten erlaubt, sofern auf diese von einem Speichermedium in den durchsuchten Räumlichkeiten zugegriffen werden kann.[633] Dadurch wird eine inhaltliche Prüfung dieser Daten ermöglicht, um zu entscheiden, ob diese aufgrund ihrer Bedeutung für das weitere Strafverfahren durch richterliche Beschlagnahme zu sichern sind. Zeitlich betrachtet stellen die Durchsuchungsvorschriften daher eine Vorstufe zur Beschlagnahme nach den §§ 94 ff. StPO dar.[634] Ziel einer Durchsicht, die im Idealfall bereits während der laufenden Durchsuchungsmaßnahme durch Techniker des LKA abgeschlossen ist, ist es, im Rahmen der Ermittlungsdurchsuchung zu bestimmen, welche Unterlagen für die Verfahrenszwecke tatsächlich relevant sind und damit förmlich beschlagnahmt werden müssen, um so eine übermäßige Datenerhebung von für das Verfahren irrelevanter Daten zu vermeiden.[635] Hierfür können die IT-Spezialisten des LKA auf den Einsatz spezieller Software zurückgreifen, die eine Durchsuchung anhand von Suchbegriffen ermöglicht.[636] Letztlich stellt § 110 StPO daher eine Norm dar, die die von der Beschlagnahme ausgehende Eingriffsintensität verringern soll.[637] Dies bringt jedoch mit sich, dass die Auswertung extern, also in Echtzeit beim Beschuldigten vor Ort und vor allem zeitlich an die Dauer der Durchsuchung geknüpft ist. Endet die Durchsuchung, so endet auch die Befugnis aus § 110 Abs. 3 StPO beim Beschuldigten vor Ort.

1) Physische Hardware

Finden die Ermittlungsbehörden vor Ort einen Datenträger auf, so können sie diesen entweder mitnehmen (vorläufige Sicherstellung) oder eine

632 *Graßie/Hiéramente*, CB 2019, 191, 192.
633 *Gercke* in: HK-StPO, § 110 StPO, Rn. 18; *Graßie/Hiéramente*, CB 2019, 191, 192; Angerer DRiZ 2019, 428, 431.
634 *Blechschmitt*, MMR 2018, 361, 363.
635 BT-Dr 16/5846, S. 63; *Graßie/Hiéramente*, CB 2019, 191, 192.
636 *Graßie/Hiéramente*, CB 2019, 191, 192.
637 BVerfGE 113, 29, 58; BVerfGE 124, 43, 72; *Beulke/Meininghaus*, StV 2007, 63, 64.

Datenkopie vor Ort fertigen.[638] Handelt es sich bei dem Gegenstand um einen mobilen Datenträger wird regelmäßig eine forensische Duplikation der Daten angefertigt. Diese Duplikation wird sodann als Arbeitsversion zum permanenten Zugriff der Ermittlungsbehörden abgespeichert und zum anderen als reine Sicherungskopie, die zum Ausschluss einer Veränderung der Metadaten unangetastet beim IT-Referenten verbleibt.[639] Da die Hardware so unter Umständen gar nicht mitgenommen werden muss, trägt dieses Vorgehen dem Verhältnismäßigkeitsgrundsatz in besonderer Weise Rechnung.[640]

2) Digitale Serverdaten

Anders stellt sich dies bei der Sicherstellung von Beweismitteln in Netzwerken dar. Es ist hier bereits aus Kapazitätsgründen regelmäßig unmöglich, das gesamte Netzwerk oder den gesamten Server vorläufig sicherzustellen. Die Unverhältnismäßigkeit eines solchen Vorgehens wäre ferner evident, wenn man sich vergegenwärtigt, dass es sich bei einem solchen Server in der Regel um den eines Dritten (häufig eines Unternehmens in Form des Dienstleistungsanbieters) handelt. Auf diesem sind neben den Daten des Betroffenen die Daten von im Zweifel Millionen anderer Personen gespeichert, die zweifelsohne unangetastet bleiben müssen.[641]

a) Entwicklung des § 110 Abs. 3 StPO

Bei § 110 Abs. 3 StPO handelt es sich um eine vergleichsweise junge Norm mit deren Kodifizierung der Gesetzgeber darauf reagierte, dass die herkömmlichen Befugnisnormen aus einer Zeit stammen, in der elektronisch gespeicherte Daten eine Seltenheit darstellten. War über lange Zeit die Aktenablage das vorherrschende Mittel zur Archivierung von Daten, werden diese heute vermehrt digital gespeichert. Als Reaktion hierauf sollten die auf physische Gegenstände in Papierform anwendbaren Vorschriften über die Gewinnung von Beweismitteln auf sämtliche Medien ausgeweitet werden, die menschliche Gedankenerklärungen und sonstige Informationen

638 *Bell*, Beschlagnahme und Akteneinsicht, S. 11 ff.
639 *Bär* in: Handbuch des Wirtschafts- und Steuerstrafrechts, Kapitel 28, Rn. 59.
640 *Greven* in: KK-StPO, § 94 StPO, Rn. 13; *Basar/Hiéramente*, NStZ 2018, 681, 682.
641 *Basar/Hiéramente*, NStZ 2018, 681, 682.

verkörpern oder speichern.[642] Im Zeitalter der fortschreitenden Digitalisierung sind es vor allem verschiedene Modelle des Cloud-Computing, auf deren neuartige Strukturen der Gesetzgeber reagieren musste. Auch im Rahmen der Sichtung der durch Sprachassistenten aufgezeichneten Daten tritt diese Problematik hervor. Die Datensichtung gelingt durch einen bloßen unmittelbaren Zugriff auf den als Durchsuchungsobjekt vorhandenen physischen Gegenstand nicht mehr. Vielmehr benötigen die Strafverfolgungsbehörden die Möglichkeit auch die auf einem virtuellen Speicher in Form eines Servers gespeicherten Unterlagen zu durchsuchen. Auf jenes Problem der dezentralen Datenspeicherung hat der Gesetzgeber mit der Erweiterung des § 110 StPO um Absatz 3 reagiert, indem die Durchsichtsmöglichkeiten auf verbundene Speichermedien erstreckt wurden.[643] § 110 Abs. 3 StPO ermächtigt mithin die Ermittlungsbehörden, sich Zugang zum Online-Account des Betroffenen zu verschaffen, um bereits während der Durchsuchung ausloten zu können, inwiefern eine förmliche Beschlagnahme überhaupt erforderlich ist.[644]

b) Voraussetzungen

aa) Allgemeines

§ 110 Abs. 3 StPO fordert für einen Online-Zugriff, die Gefahr des drohenden Datenverlusts. Die Gefahr darf nicht bloß behauptet werden, vielmehr müssen konkrete Anhaltspunkte vorliegen.[645] Mit entscheidend ist in diesem Zusammenhang, ob der Nutzer in der Lage ist, einen irreversiblen Datenverlust beim Dienstleistungsanbieter herbeizuführen. Es wird hinsichtlich Sprachassistenzsysteme zur Bejahung konkreter Anhaltspunkte für eine solche Gefahr jedoch bereits ausreichend sein, dass der Betroffene die Möglichkeit hat, gespeicherte Cloud-Inhalte zu löschen.[646] Sowie ein Tatverdächtigter von dem geplanten Zugriff auf seine Daten beim Dienstleistungsanbieter erfahren würde, würde er seinen zeitlichen Vorsprung

642 *Obenhaus*, NJW 2010, 651, 651.
643 Vgl. BS-Drs. 19/11478 als Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Stephan Thomae, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP, S. 3; *Bär*, ZIS 2011, 53, 54.
644 *Wolter* in: SK-StPO, § 110 StPO, Rn. 6; *Graßie/Hiéramente*, CB 2019, 191, 192.
645 *Park*, Durchsuchung und Beschlagnahme, Rn. 823.
646 Vgl. https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (zuletzt abgerufen am 31.10.2021).

nutzen, um mögliche ihn belastenden Aufzeichnungen über seinen Account zu löschen. Um § 110 Abs. 3 StPO nicht seines Sinnes zu berauben, darf keine konkrete Zugriffsmöglichkeit im Zeitpunkt der Durchsuchung auf die gesondert gespeicherten Daten gefordert werden. Eine abstrakte Zugriffsmöglichkeit muss in diesen Fällen genügen.[647] In Extremfällen käme man ansonsten zu dem verwunderlichen Ergebnis, dass sich der Betroffene durch einen defekten Computer oder einer im Moment der Durchsuchung nicht vorhandenen Internetverbindung der Durchsicht entziehen könnte.[648] Erforderlich ist lediglich, dass ein Zugriff auf die räumlich getrennten Speichermedien mit den lokalen informationstechnischen Systemen möglich ist.[649] Insofern ist bei Sprachassistenten zu beachten, dass im Unterschied zu Fällen des herkömmlichen Cloud-Storage (bspw. Dropbox), in denen direkt über das informationstechnische Endgerät in Form einer Desktopanwendung die Durchsicht der gespeicherten Daten erfolgen kann, dies beim Sprachassistenten nicht unmittelbar über das informationstechnische Endgerät möglich ist. Vielmehr ist mittels der Zugangsdaten über einen Computer eine Anmeldung bei dem beim Dienstleistungsanbieter hinterlegten Account erforderlich, um auf das räumliche getrennte Speichermedium in Form des Servers zugreifen zu können. Dies hindert die Anwendung der Vorschrift auf Sprachassistenten jedoch mitnichten.[650] Denn es muss lediglich mittels eines von der Durchsuchung betroffenen Systems auf die Cloudserver zugegriffen werden können.[651] Für die Praxis ist daher entscheidend, dass im Durchsuchungsbeschluss die räumlich getrennten Speichermedien, auf die sich die Durchsicht beziehen kann, wenigstens gegenständlich beschrieben werden.[652]

---

647 *Brodowski/Eisenmenger,* ZD 2014, 119, 122; *Park*, Durchsuchung und Beschlagnahme, Rn. 825.

648 *Brodowski/Eisenmenger,* ZD 2014, 119, 122.

649 *Gercke* in: HK-StPO, § 110 StPO, Rn. 18.

650 Vgl. den Verweis auf „digitale Assistenten wie „Alexa" (Amazon), „Siri" (Apple), „Cortana" und „Hello" (Microsoft und Google)" *Bruns* in: KK-StPO, § 110 StPO, Rn. 8.

651 *Wicker*, MMR 2013, 765, 767.

652 *Herrmann/Soiné,* NJW 2011, 2922, 2925; *Knierim*, StV 2009, 206, 211; vertiefend vgl. *Hiéramente*, wistra 2016, 432, 433; zu den Anforderungen vgl. aktuell BGH, Beschluss vom 09.02.2021 – StB 9/20, StB 10/20; a.A.: *Ladiges* in: Radtke/Hohmann, § 110 StPO, Rn. 16.

bb) Möglichkeiten der Sichtung

Die Sichtung ist für die Ermittlungsbeamten auf verschiedenen Wegen durchführbar. Über seinen Wortlaut hinaus, der eine Wegnahme des durchsuchten Gegenstandes oder Datenträgers nicht vorsieht, ist § 110 StPO im Hinblick der Gewährleistung einer effektiven und gründlichen Durchsicht weit zu verstehen, sodass auch eine Mitnahme des Datenträgers möglich ist (vorläufige Sicherstellung).[653] In diesem Fall haben die Ermittlungsbeamten schließlich gem. § 98 Abs. 2 S. 1 StPO innerhalb von drei Tagen die richterliche Bestätigung der vorläufigen Sicherstellung zu beantragen. Die Durchsicht hat sodann unter Beachtung des Verhältnismäßigkeitsgrundsatzes und der konkreten Umstände des Einzelfalles zügig zu erfolgen, muss aber – auch in der gerichtlichen Bestätigung – nicht ausdrücklich befristet werden.[654]

Bezüglich eines Smart Speaker ist an dieser Stelle jedoch problematisch, dass die Mitnahme des vermeintlichen Datenträgers in Form des Endgeräts keinen Mehrwert darstellen würde, da hierauf keine gespeicherten Inhalte zu finden sind.[655] Zur Sichtung der aufgezeichneten Daten sind lediglich die Zugangsdaten zum Account des Betroffenen entscheidend. Um dem Betroffenen die Möglichkeit zu nehmen, sich nach der erfolgten Durchsuchung selbst in seinem Account einzuloggen und entsprechende Aufnahmen zu löschen, stellt sich die Frage, ob die Strafverfolgungsbehörden auch ermächtigt sind, die Zugangsdaten temporär zu ändern oder wenigstens eine virtuelle Versiegelung anzubringen. Ob dies im Sinne einer effektiven Strafverfolgung möglich ist, dürfte letztlich eine Frage der Verhältnismäßigkeit, insbesondere eine solche der Erforderlichkeit, darstellen. Hinsichtlich milderer Mittel ist vor allem an eine Sicherungskopie zu denken, vgl. § 110 Abs. 3 S. 2 StPO. Dadurch wird der zum Zeitpunkt der Durchsuchung vorhandene Datenbestand eingefroren und ein Beweismittelverlust ist nicht zu befürchten. Insbesondere wird durch ein derartiges Vorgehen auch vermieden, dass die Strafverfolgungsbehörden im Rahmen der Sichtung zu späteren Zeitpunkten mehrere Male immer wieder unmit-

653 BGH, NStZ 2003, 670, 671; *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 2; *Hegmann* in: BeckOK-StPO, § 110 StPO, Rn. 8; *Bruns* in: KK-StPO, § 110 StPO, Rn. 9.

654 BGH, Beschluss. v. 20.–5.2021 – StB 21/21; BGH, NStZ 2003. 671, 671.

655 Zur Frage, ob ein Datenträger bzw. die Hardware, auf der unmittelbar potenzielles Beweismaterial gespeichert ist zur Durchsicht auf Grundlage des § 110 StPO ohne Beschlagnahme mitgenommen werden darf, vgl. *Liebig*, Der Zugriff auf Computerinhaltsdaten, S. 35 ff.

telbar auf den Server zugreifen und dabei womöglich auch neue, nach der durchgeführten Durchsuchung, aufgezeichnete Nachrichten einsehen. Ein solches Vorgehen wäre nicht durch die Befugnisnorm des § 110 StPO gedeckt, da diese lediglich den einmaligen, punktuellen Zugriff auf ein Speichermedium erlaubt.[656] Nach Erstellen der Sicherungskopie darf daher keine Verbindung mehr zum Server aufgebaut werden. Ansonsten würden die Grenzen zur Online-Durchsuchung verwischt, da jeder weitere Zugriff auf räumlich getrennte Speichermedien keine bloße Durchsicht, sondern eine Überwachung darstellen würde.[657] Dieses Vorgehen ist für den Betroffenen bedeutend milder als die mit einer Beschlagnahme einhergehende Entziehung der Nutzungsmöglichkeiten des entsprechenden Gegenstandes oder im Falle elektronischer Daten einer anzudenken Zugangssperre, sodass dadurch dem Verhältnismäßigkeitsgrundsatz in besonderer Weise genügt wird.[658] Die Beachtung des Verhältnismäßigkeitsgrundsatzes einer Sichtung nach § 110 Abs. 3 StPO weiter unterstreichend, kann zudem bereits in der Durchsuchungsanordnung nach § 105 StPO der Zeitraum aus welchem Aufzeichnungen Gegenstand einer Sicherungskopie sein sollen zeitlich begrenzt werden. Erhoffen sich die Ermittler Erkenntnisse zu einer konkreten Mordnacht so wird es in der Regel ausreichend sein, die Aufzeichnungen weniger Tage vor und nach dem Tattag zu sichten. Unabhängig von der technisch bedingten Sinnlosigkeit das Endgerät des Sprachassistenten als physische Hardware sicherzustellen, scheidet wie dargelegt auch die (vorläufige) Sicherstellung des kompletten Servers aus Verhältnismäßigkeitsgesichtspunkten aus. Stattdessen muss die Sichtung mittels eines unmittelbaren Zugriffs auf die konkreten Daten des Betroffenen vorgenommen werden (sog. Live-Forensik[659], während das betroffenen System noch „online" ist, daher noch läuft). Problematisch dabei ist, dass mit einem solchen unmittelbaren Zugriff stets Veränderungen im System einhergehen, wodurch die sog. Metadaten verwischt werden können.[660] Im Übrigen kann auch die sog. Live-Forensik das Problem nicht lösen, dass keine ausreichende Vorsortierung der zu sichernden Daten möglich ist.

656 *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 6; *Zerbes / El-Ghazi*, NStZ 2015, 425, 432.

657 *Brodowski/Eisenmenger,* ZD 2014, 119, 125.

658 BT-Drs. 16/5846, S. 63.

659 Vgl. *Heinson*, IT-Forensik, S. 37; BSI Leitfaden „IT – Forensik", 2011, S. 13, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 31.10.2021).

660 *Basar/Hiéramente*, NStZ 2018, 681, 682.

Aufgrund der zeitlichen und ressourcentechnischen Umstände bei einer Durchsuchung, ist oftmals lediglich die Sicherung ganzer Verzeichnisse umsetzbar, was regelmäßig eine breitflächige Sicherung verfahrensirrelevanter Daten bedeutet.[661] Gleichwohl darf auf eine sorgfältige Durchsicht zum Ziel der Aussonderung nicht beweisrelevanter Daten nicht mit dem Argument verzichtet werden, dass der auf einem Datenträger gespeicherte Datenbestand ein einziges Beweismittel sei.[662] Beweismittel ist stets der konkrete Inhalt sowie die Metadaten der Dateien, nicht jedoch der gesamte Datenträger hinsichtlich der sich darauf befindlichen Dateien.[663] Allein der Umstand, dass potentiell beweisrelevante Daten auf einem Server gespeichert sind, legitimiert ferner nicht dazu, den gesamten Datenbestand des Serverlaufwerks zu kopieren.[664]

cc) Möglichkeiten zur Passworterlangung

Um den Accountzugriff zu ermöglichen, ergibt sich aus § 110 Abs. 3 StPO jedoch keine Verpflichtung für den von der Durchsuchung Betroffenen, den Ermittlungsbehörden den Zugriff auf einen solchen Account durch die Herausgabe möglicher Passwörter zu ermöglichen.[665] Unter Zugrundelegung des nemo-tenetur Grundsatzes muss der Beschuldigte sich an seiner eigenen Überführung nicht aktiv beteiligen.[666] Der nemo-tenetur-Grundsatz ist als Ausdruck der uneingeschränkten rechtsstaatlichen Achtung der Menschenwürde in Art. 20 Abs. 3 GG verankert und verbietet es den Beschuldigten zu zwingen, aktiv an seiner Überführung mitzuwirken.[667] Ob und inwieweit der Beschuldigte im Strafverfahren mitwirkt, muss er – nicht zuletzt aufgrund seiner verfassungsrechtlichen Stellung als Verfahrensbeteiligter und nicht bloßes Objekt des Verfahrens – selbstbestimmt entscheiden können.[668] Ebenso hat daher ein zwangsweises Hinwirken

661 *Basar/Hiéramente*, NStZ 2018, 681, 683.
662 BVerfGE 113, 29, 61.
663 *Szesny*, WiJ 2012, 228, 231.
664 *Szesny*, WiJ 2012, 228, 231.
665 *Obenhaus*, NJW 2010, 651, 652 f.
666 *Neuhaus*, StV 2020, 489, 490; *Rottmeier/Eckel*, NStZ 2020, 193, 199.
667 BVerfG, NJW 2013, 1058, 1061; *Momsen*, DRiZ 2018, 140, 141.
668 BVerfG, NJW 2013, 1058, 1061; ebenso zählt der Grundsatz der Selbstbelastungsfreiheit zum Kern des von Art. 6 EMRK garantierten Rechts auf ein faires Strafverfahren schützt den Beschuldigten gegen unzulässige Zwangs- und Druckausübung seitens der Strafverfolgungsbehörden, vgl. EGMR, StV 2003,

auf die Preisgabe der Daten gem. § 136a Abs. 1 StPO zu unterbleiben.[669] Sofern die Zugangsdaten nicht freiwillig herausgegeben werden, kommen für die Strafverfolgungsbehörden verschiedene Möglichkeiten in Betracht.

(1) Technische Entschlüsselung

Naheliegend ist der Versuch einer technischen Entschlüsselung. Bereits in der Gesetzesbegründung heißt es hierzu, dass sich die Strafverfolgungsbehörden zwar nicht mittels eines heimlichen staatlichen Hackerangriffes Zugang zum gesicherten Server verschaffen dürfen, die Durchsuchung und damit auch die Möglichkeit der Datensichtung jedoch zwangsweise durchsetzbar bleiben muss.[670] Dies bedeutet, dass nachdem der Betroffene die Herausgabe der Zugangsdaten verweigert hat, es den Ermittlungsbeamten gestattet ist, mittels einer Software das vom Betroffenen benutzte technische System nach den hier zwischengespeicherten Passwörtern zu durchleuchten.[671] Eine Möglichkeit stellt in diesem Kontext die die „Brute-Force"-Methode dar, mittels derer durch das Ausprobieren aller möglichen Passwortkombinationen die Zugangsdaten errechnet werden können.[672] Um die für diese Berechnungsprozesse notwendige Rechnerleistung zu minimieren und die Entschlüsselung zu beschleunigen, können alle auf dem Computer gespeicherten Worte indiziert werden und die Entschlüsselungsversuche im Rahmen der Brute-Force-Methode auf die in diesem

257, 259; zu den verfassungsrechtlichen Grundlagen des Nemo-tenetur Grundsatzes vgl. *Böse*, GA 2002, 98 ff.

669 *Bäumerich*, NJW 2017, 2718, 2720; *Gercke*, MMR 2008, 291, 298; *Gerhards*, Recht auf Verschlüsselung, S. 294 f.

670 BT-Dr 16/5846, S. 64.

671 *Zerbes/El-Ghazi*, NStZ 2015, 425, 432; *Peters*, NZWiSt 2017, 465, 467.

672 *Hegmann* in: BeckOK-StPO, § 110 StPO, Rn. 18. Dabei ist jedoch zu berücksichtigen, dass für ein solches Vorgehen große Rechnerleistungen erforderlich sind. Bereits ein handelsüblicher Computer bräuchte beispielsweise für das Herausfinden eines komplexen achtstelligen Passworts mit Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen ca. 83 Tage. Besteht das Passwort hingegen lediglich aus Kleinbuchstaben, nimmt der entsprechende Prozess nur noch 35 Minuten in Anspruch. Trotz dieser unter Umständen erheblichen Zeitspanne ist zu berücksichtigen, dass den Strafverfolgungsbehörden in der Regel hochleistungsfähige Computer zur Verfügung stehen, das korrekte Passwort nicht erst als letzte denkbare Alternative herausgefunden wird und die Betroffenen nicht immer ein komplexes Passwort verwenden werden, vgl. *Grözinger*, Die Überwachung von Cloud-Storage, nach BSI, IT-Grundschutz, S. 50.

Index enthaltenen Wörter beschränkt werden bzw. um entsprechende Mutationen (z. B. mit Zahlen oder Sonderzeichen, Groß-, Kleinschreibung) ergänzt werden.[673] Nach anderer Auffassung soll dies angesichts des Umstandes, dass damit ein gravierender, verdeckter (Begleit-)Eingriff in die Integrität des externen informationstechnischen Systems einhergehe, nicht erlaubt sein.[674] Es bliebe allenfalls die Möglichkeit dass die Ermittler die Zugangsdaten selbst – als zwischengestaltete menschliche Aktion – eingeben, nachdem diese beispielsweise in den Unterlagen des Betroffenen während einer Durchsuchung aufgefunden wurden.[675] Nur auf diese Weise könnten die Zugangshindernisse des Servers auf dem dafür vorgesehen Wege und damit rechtmäßig aufgehoben werden. Dafür, dass jedoch darüber hinausgehend auch der Einsatz entsprechender technischer Mittel zur Kenntniserlangung der Zugangsdaten als „Annexkompetenz" von § 110 Abs. 3 StPO umfasst sein muss, spricht, dass auch im Rahmen der Durchsuchung nach § 102 StPO gefundene Behältnis aufgebrochen werden dürfen.[676] Ob ein physisches oder virtuelles Zugangshindernis durchbrochen wird, kann dabei keinen Unterschied machen.

(2) Bestandsdatenabfrage gem. § 100j StPO

Zudem käme in Betracht die Zugangsdaten im Rahmen einer Nutzungs- und Bestandsdatenabfrage gem. § 100j StPO beim Dienstleistungsanbieter zu erfragen.[677] Die im Zuge der Änderung des Telekommunikationsgesetzes zum 01.07.2013 in Kraft getretene Vorschrift,[678] ermöglicht es von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des TKG erhobenen Daten zu verlangen. Gem. § 113 Abs. 1 S. 2 TKG[679] gilt

673 *Willer/Hoppen*, CR 2007, 610, 615.
674 *Brodowski/Eisenmenger,* ZD 2014, 119, 123.
675 *Brodowski/Eisenmenger,* ZD 2014, 119, 123.
676 *Obenhaus*, NJW 2010, 651, 653; *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 6.
677 *Krause*, Kriminalistik 2014, 213, 214.
678 *Bruns* in: KK-StPO, § 100j StPO, Rn. 1.
679 Nach BVerfG, NJW 2020, 2699, Rn. 134 ff., ist § 113 TKG überdies verfassungswidrig, da die auf alleiniger Grundlage des § 113 TKG erfolgte Bestandsdatenabfrage nicht den Grundsätzen der Verhältnismäßigkeit genügt. Der Norm fehlt es an normierten Eingriffsschwellen, die sicherstellen, dass Auskünfte nur bei einem auf tatsächliche Anhaltspunkte gestützten Anlass eingeholt werden

dies theoretisch auch für die hier gefragten Zugangssicherungscodes.[680] In Anbetracht dessen, dass die Server des Sprachassistenten räumlich getrennte Speichermedien des Endgeräts darstellen, scheint die Vorschrift wie geschaffen für die hiesige Situation. Dies zeigen auch die Gesetzgebungsmaterialien, nach denen die Vorschrift auf Vorgänge des Cloud Computing Anwendung finden soll.[681] Dem gesetzgeberische Willen nach sollte durch die Neuregelung des § 100j StPO am Beispiel des Cloud-Computing durch die Herausgabe der Zugangsdaten ein Zugang zu extern abgespeicherten Daten ermöglicht werden.[682] Dabei ist zu beachten, dass Voraussetzung für eine Abfrage, die einen Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, darstellt, das Vorliegen der gesetzlichen Voraussetzungen für die beabsichtige Form der Nutzung der Zugangsdaten notwendig ist, § 100j Abs. 1 S. 2 StPO.[683] Soll heimliche laufende Telekommunikation überwacht werden, müssen die Voraussetzungen des § 100a StPO vorliegen, sollen archivierte Daten öffentlich durchsucht oder beschlagnahmt werden, müssen regelmäßig die Voraussetzung einer Durchsuchung gem. §§ 102 ff. StPO oder einer Beschlagnahme nach §§ 94 ff. StPO vorliegen.[684] Bezogen auf Cloud-Computing in Form der Nutzung eines Smart Speakers muss § 100a StPO als Rechtsgrundlage jedoch ausscheiden, da dessen Nutzung keine Telekommunikation im Rahmen des § 100a StPO darstellt. Bleiben noch mögliche offenen Ermittlungsbefugnisse. Gegen eine Heranziehung der §§ 94 ff. StPO wird vorgebracht, dass die Passwort Herausgabe und die anschließende Durchsuchung der Cloud nur heimlich erfolgen könne, da der Betroffene ansonsten, sobald er von der Maßnahme Kenntnis erlangt, sein Passwort ändern und belastende Inhalte löschen würde.[685] Dem ist insofern zuzustimmen, dass bei Durchführung der Bestandsdatenauskunft eine Verzögerung zwischen Anfrage und Durchsuchung eintritt, in welcher der Beschuldigte womöglich belastende Aufzeichnungen löschen könnte. Allerdings ist

können. Hinsichtlich der Strafverfolgung ist diesbezüglich wenigstens das Vorliegen eines Anfangsverdachts erforderlich.

680 *Schnabel*, CR 2012, 253, 255.

681 BR-Drs. 664/1/12, S. 13 f.

682 *Graf* in: BeckOK-StPO, § 100j StPO, Rn. 23; *Bär*, MMR 2013, 700, 702; *Bruns* in: KK-StPO, § 100j StPO, Rn. 7; *Dalby*, CR 2013, 361, 363.

683 BT-Drs. 17/12034, S. 13; *Burhoff*, StRR 2015, 8, 9; im Unterschied zu § 113 TKG normiert § 100j Abs. 1 S. 2 StPO damit gesetzliche Eingriffsschwellen.

684 *Keller* in: HH-Ko/MedienR, Abschnitt 90, Rn. 24; *Hauck*, StV 2014, 360, 362.

685 *Dalby*, CR 2013, 361, 368.

nicht vorgeschrieben, dass der Betroffene unmittelbar von der Bestandsdatenabfrage zu informieren ist. Vielmehr ist gem. § 100j Abs. 4 S. 2 StPO die Benachrichtigung erst dann vorzunehmen, wenn hierdurch der Zweck der Auskunft nicht mehr vereitelt würde. Daher ist es gesetzeskonform, eine zunächst heimliche Bestandsdatenabfrage durchzuführen, um sodann in Kenntnis der Passwörter den Beschuldigten aufzusuchen und über dessen technische Geräte eine offene Durchsuchung seiner Cloud durchzuführen. Durch eine heimliche Bestandsdatenauskunft verliert die sich anschließende Durchsuchung nicht ihren Charakter als offene Ermittlungsbefugnis, sofern jedenfalls sie selbst offen durchgeführt wird. Somit bleibt § 94 StPO als Rechtsgrundlage für das Zugreifen auf Cloud-Inhalte im Zusammenspiel mit § 100j Abs. 1 S. 2 StPO erhalten.

Problematisch ist jedoch, ob der Cloud-Anbieter überhaupt als Verpflichteter des § 100j StPO angesehen werden kann.[686] Voraussetzung wäre, dass dieser eine Telekommunikationsdienstleistung erbringt oder an einer solchen mitwirkt. Da bereits § 100j StPO auf das Telekommunikationsgesetz verweist und die Bestandsdatenabfrage mit den dortigen Vorschriften kohäriert, müsste der Cloud-Anbieter daher eine Telekommunikationsdienstleistung im Sinne des Telekommunikationsgesetzes erbringen.[687] Dies sind gem. § 3 Nr. 24 TGK in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über TK-Netze bestehen. Hinsichtlich der Übertragung der Audioaufzeichnungen in die Cloud handelt es sich dabei zweifelsohne um einen solchen Datentransportvorgang im Sinne des TKG. Allerdings wird dieser Übertragungsvorgang gerade nicht vom Cloud-Anbieter, sondern dem Access-Provider, der das Internet bereitstellt, erbracht.[688] Der Cloud-Dienstleister stellt lediglich die Schnittstellen bereit, um die Inhalte nach der Übertragung in die Cloud als Rechenzentrum zu verbringen. Der Transport, mithin die Übertragung der Inhalte als solche, erfolgt dabei vorgelagert durch den von ihm genutzten Transportdienstleister (den Access-Provider), der unabhängig von dem Cloud Dienstleister fungiert.[689] Nur der Access-Provider erbringt daher eine Leistung, die in der Übertragung von Signalen besteht. Dieser Übermittlungsvorgang durch den Access-Provider erfolgt vollständig losgelöst von der Leistungserbringung

686 vgl. auch *Wicker*, MMR 2014, 298, 300.
687 *Wicker*, MMR 2014, 298, 300; *Boos/Kroschwald/Wicker*, ZD 2013, 205, 206.
688 *Wicker*, MMR 2014, 298, 300; *Boos/Kroschwald/Wicker*, ZD 2013, 205, 206.
689 *Kremer/Völkel*, CR 2015, 501, 503.

zwischen Cloud Service und Nutzer.[690] Anbieter von Clouddienstleistungen sind daher nicht mit Telekommunikationsdienstleistern gleichzusetzen.[691] Da Anbieter von Clouddienstleistungen mithin keine Anbieter von Telekommunikationsdienstleistungen sind, sind sie auch nicht Adressat eines Auskunftsverlangens nach § 100j StPO.[692] Um auf § 100j StPO zurückzukommen, kann diese Norm daher nur eine Auskunftsanfrage bei dem Access-Provider (bspw. Deutsche Telekom, 1&1, Freenet oder Vodafone) als Telekommunikationsanbieter legitimieren, die zwar rechtlich zulässig, in der Praxis jedoch nicht zielführend sein wird. Der Telekommunikationsdienstleister kann lediglich Auskunft über Bestandsdaten im Sinne der § 95 und 111 TKG geben, worunter Rufnummern, der Name und die Anschrift des Anschlussinhabers oder das Datum des Vertragsbeginns fallen. Nicht hierunter fallen jedoch Bestandsdaten des Cloud-Nutzers beim Cloud-Anbieter. Diese durch den Cloud-Anbieter erhobenen Bestandsdaten werden stattdessen durch § 14 TMG erfasst, wonach der Telemedienanbieter (daher Apple, Amazon oder Google) personenbezogene Daten eines Nutzers "*erheben und verwenden [darf], soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind*". Diese Bestandsdaten und vor allem die Nutzungsdaten in Form der Merkmale zur Identifikation des Nutzers nach § 15 Abs. 1 Nr. 1 TMG, worunter auch die Zugangsdaten fallen[693], liegen wiederum dem von § 100j StPO erfassten Access-Provider nicht vor, da sie nur vom Cloud-Anbieter als Telemedienanbieter erhoben werden können.[694] Somit hat der Telekommunikationsdienstleister, der die entsprechende Dienst-

690 *Boos/Kroschwald/Wicker*, ZD 2013, 205, 206.

691 *Eschelbach* in: SSW-StPO, § 100j StPO, Rn. 10; *Grünwald/Döpkens*, MMR 2011, 287, 288.

692 *Gercke* in: HK-StPO, § 100j StPO, Rn. 6; *Greco* in: SK-StPO, § 100j StPO, Rn. 11; *Hauck* in: LR-StPO, § 100j StPO, Rn. 15a; *Wicker*, MMR 2014, 298, 300; *Boos/Kroschwald/Wicker*, ZD 2013, 205, 206; *Bedner*, Cloud Computing, S. 115; *Bunzel*, Der strafprozessuale Zugriff auf IT-Systeme, S. 367 f.; *Zimmermann*, JA 2014, 321, 326; *Schuster/Reichl*, CR 2010, 38, 43; a.A., jedoch ohne eingehende Begründung und mit bloßem Verweis auf die Gesetzgebungsmaterialien: *Köhler* in: Meyer-Goßner/Schmitt, § 100j StPO, Rn. 3; *Bär*, MMR 2013, 700, 702; *Bruns* in: KK-StPO, § 100j StPO, Rn. 7; *Dalby*, CR 2013, 361, 363.

693 *Schreibauer* in: Auernhammer-DSGVO/BDSG, § 15 TMG, Rn. 7; *Zscherpe* in: Taeger/Gabel-BDSG, § 15 TMG, Rn. 17.

694 *Wicker*, MMR 2014, 298, 300 f.; *dies*., Cloud-Computing und staatlicher Strafanspruch, S. 389.

leistung nicht selbst erbringt, keine Kenntnis der Zugangsdaten und kann diese folglich auch nicht herausgeben.[695][696]

(3) Auskunftsverlangen gem. §§ 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG

Da es sich bei den Cloud-Anbietern zwar um Anbieter von Informations- und Kommunikationsdiensten handelt, diese aber gleichzeitig keine Telekommunikationsdienstleister darstellen, sind diese aufgrund der Negativformulierung in § 1 TMG als Telemediendienstanbieter anzusehen.[697] Telemediendienste leisten mehr als die bloße Signalübertragung über ein Telekommunikationsnetz.[698] Insbesondere Clouddienste mit Software-as-a-Service, Function-as-a-Service oder auch Plattform-as-a-Service Anwendungen, sind aufgrund ihrer Bereitstellung der genutzten Software als Telemedienanbieter einzuordnen. Schließlich wird dabei nicht die Signalübertragung übernommen, sondern wie auch im Falle von Sprachassistenten das komplette Management von entfernten Infrastrukturen und Ressourcen.[699] Eine Ausnahme könnte allenfalls dann anzudenken sein, wenn der Cloud-Anbieter zugleich Leistungen eines Access-Providers erbringt (d.h. das zur Verfügung stellen eines eigenen selbst betriebenen Zugangsdienstes) und seinen Nutzern so ein kompletten Netzwerk-as-a-Service Dienst zur Verfügung stellt.[700] Jedoch sind bei der Nutzung eines Smart Speakers der geläufigen Marken Amazon oder Google der Internetzugang einerseits und die Cloud Computing-Dienste anderseits technisch unabhängige Leistungen und werden von separaten Anbietern erbracht. Während der Internetzugang durch den Accesprovider bzw. Telekommunikationsdienstleister erbracht wird, erfolgt die Verarbeitung der Sprachbefehle in der Cloud durch Amazon oder Google als Telemediendienstanbieter. Daher könn-

695 *Hartmann* in: HK-GS, § 100j StPO, Rn. 11; *Wicker*, MMR 2014, 298, 302.
696 Zur Einschlägigkeit des § 100j StPO bzgl. eines E-Mail-Providers, vgl. *Redeker* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 12, Rn. 217 ff.
697 So *Hauck* in: LR-StPO, § 100j StPO, Rn. 15a; *Greco* in: SK-StPO, § 100j StPO, Rn. 11; *Nolte* in: Borges/Meents Cloud-Computing, § 11 Rn. 24 f. m.w.N. zur Ansicht, ob das TMG auf Cloud-Dienste generell keine Anwendung finden soll.
698 *Martini* in: BeckOK-InfoMedienR, § 1 TMG, Rn. 11; vgl. auch OLG München, MMR 2019, 532, Rn. 61.
699 *Bedner*, Cloud Computing, S. 116; *Müller*, Cloud Computing, S. 221; *Boos/Kroschwald/Wicker*, ZD 2013, 205; vgl. auch BT-Drs. 16/3078, S. 13.
700 *Kremer/Völkel*, CR 2015, 501, 505; *Müller*, Cloud Computing, S. 197.

ten die Strafverfolgungsbehörden ihr Auskunftsverlangen auf §§ 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG stützen. § 14 Abs. 2 TMG besagt, dass *„auf Anordnung der zuständigen Stellen […] der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen [darf], soweit dies für Zwecke der Strafverfolgung […] erforderlich ist"*. Gem. § 15 Abs. 5 S. 4 TMG ist diese Vorschrift auf die Auskunftserteilung hinsichtlich Nutzungsdaten ebenfalls anzuwenden. Die §§ 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG enthalten allerdings keine Befugnis der öffentlichen Stellen zum Auskunftsverlangen, sondern bestimmen lediglich den Umfang und Zweck der Übermittlungsbefugnis des Dienstanbieters.[701] Dies folgt unmittelbar aus der Formulierung des § 14 Abs. 2 TMG, der von „darf" und nicht wie § 100j StPO davon spricht, dass die Behörden berechtigt sind, eine Sache zu verlangen. Eine solche Befugnisnorm wie § 100j StPO, die auf entsprechende Vorschriften des TMG verweist, findet sich nicht. Auch nach dem Willen des Gesetzgebers stellt § 14 Abs. 2 TMG keine Ermächtigungsvorschrift da, sondern soll lediglich sicherstellen, dass der Telemedienanbieter an ihn herangetragene Auskunftsansprüche nicht aus datenschutzrechtlichen Gründen zurückweist.[702] Stattdessen liegt die datenschutzrechtliche Verantwortung hinsichtlich der Zulässigkeit der Datenübermittlung bei der anordnenden öffentlichen Stelle.[703] Es ist daher erforderlich, dass das Auskunftsverlangen auf eine entsprechende spezialgesetzliche Erhebungsbefugnis auf Seiten der Sicherheitsbehörden gestützt wird.[704] Als solche Befugnis wird teilweise § 95 Abs. 1 StPO[705] oder auch § 161 StPO[706] bemüht.

Für die Anwendbarkeit des § 14 Abs. 2 TMG auf Cloud-Anbieter kann schließlich offenbleiben, ob der Gesetzgeber Cloud-Dienstleistungsanbieter fälschlicherweise als Telekommunikationsdienstleister einordnete oder die durch die Existenz des TMG erforderliche Differenzierung zwischen Telekommunikationsdienstleitern und Telemediendienstleistern verkannte. Zwar ging der Gesetzgeber ausweislich der Gesetzgebungsmaterialien davon aus mit der Kodifizierung des § 100j StPO explizit Fälle des Cloud-Computing zu regeln, doch ändert dies nichts an der Unanwendbarkeit der §§ 95, 111, 113 Abs. 1 S. 2 TKG auf den Cloud-Dienstleister. Ein Auskunftsanspruch könnte sich lediglich nach § 15 Abs. 5 S. 4 TMG i.V.m.

701 *Karg*, DuD 2015, 85, 87.
702 *Zscherpe* in: Taeger/Gabel-BDSG, § 14 TMG, Rn. 42.
703 BS-Drs. 16/3078, S. 16.
704 *Zscherpe* in: Taeger/Gabel-BDSG, § 14 TMG, Rn. 42; *Karg*, DuD 2015, 85, 87; *Hoeren*, NJW 2007, 801, 805.
705 *Kipker/Voskamp*, ZD 2013, 119, 120 f.
706 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 406 f.

§ 14 Abs. 2 TMG und den spezialgesetzlichen strafprozessualen Vorschriften richten. Gegen eine Heranziehung der Generalklausel des § 161 StPO spricht entschieden, dass aufgrund der gewichtigen Bedeutung der Nutzungsdaten in Form der Zugangssicherungscodes der mit deren Erhebung verbundenen Eingriff in Art. 10 GG durch die Generalklausel nicht zu rechtfertigen ist.[707] Es blieben somit wiederum die §§ 94 ff. StPO deren praktische Anwendung allerdings ebenfalls an einer technisch bedingten Grenze scheitern. Aus Gründen der Datensicherheit speichert ein Großteil der Dienstleistungsanbieter die Passwörter nicht im Klartext, sondern verschlüsselt.[708] Sodann besitzt der Telemedienanbieter selbst nur einen sog. Hashwert[709], hat aber keine Kenntnis des Passwortes.[710] Da der Telemedienanbieter das Passwort daher nicht im Sinne des Telemediengesetzes im Klartext erhoben hat, kann er dieses auch nicht an die Strafverfolgungsbehörden herausgeben.[711]

(4) Zwischenergebnis

Zur Passworterlangung scheidet daher ein Vorgehen gegen den Cloud-Anbieter nach § 100j StPO i.V.m. §§ 95, 111, 113 Abs. 1 S. 2 TKG aus, da dieser nicht Verpflichteter des Anspruchs ist. Ein Auskunftsverlangen nach § 15 Abs. 5 S. 4 TMG i.V.m. § 14 Abs. 2 TMG i.V.m. §§ 94 ff. StPO scheitert in der Regel daran, dass der Cloud-Dienstleistungsanbieter das Passwort faktisch mangels Kenntnis nicht herausgeben kann. Es kommt daher nur der Einsatz eines Keyloggers oder anderweitiger Cracking-Tools in Betracht.[712] Insbesondere ist diese Vorgehensweise mangels Einschlägigkeit des § 100j StPO zur Bestandsdatenauskunft beim Cloud-Anbieter,

707 *Karg*, DuD 2015, 85, 88; *Bunzel*, Der strafprozessuale Zugriff auf IT-Systeme, S. 370.

708 BVerfG, NJW 2020, 2699, 2700.

709 Hashwert bezeichnet im Bereich der Computertechnik eine Verschlüsselung, die mittels eines Algorithmus errechnet wird und einem bestimmten Datensatz zugeordnet ist. Der ursprüngliche Inhalt der Datei kann damit nicht rekonstruiert werden, vgl. *Grützner/Jakob*, Compliance von A-Z, Hashwert(-funktion).

710 Vgl. BR-Drs. 664/1/12, S. 14.

711 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 406; *Grözinger*, Die Überwachung von Cloud-Storage, S. 247.

712 In technischer Hinsicht ermöglicht das Keylogging die Protokollierung aller Tastenanschläge, wodurch die verwendeten Passwörter nachvollzogen werden können, vgl. *Skistims/Roßnagel*, ZD 2012, 3, 5; *Fox*, DuD 2007, 827, 830; *Bunzel*, Der strafprozessuale Zugriff auf IT-Systeme, S. 69.

nicht durch die vermeintlich abschließende Regelung in § 100j StPO ausgeschlossen.[713]

3) § 110 Abs. 3 StPO im Verhältnis zum Dienstleistungsanbieter

Im Zusammenhang mit einem Vorgehen nach § 110 Abs. 3 StPO wird vereinzelt als problematisch erachtet, dass es sich dabei zwar gegenüber dem Betroffenen um eine offene Maßnahme handelt, der Dienstleistungsanbieter und Betreiber der Cloud im Stadium der Datensichtung jedoch keine Kenntnis der auf dem eigenen Server ablaufenden staatlichen Sichtung hat. Ihm gegenüber handelt es sich um einen heimlichen Eingriff.[714] Da den Strafverfolgungsbehörden durch ihre Ermittlungen jedoch nur die Zugangsdaten zum Account des tatverdächtigen Betroffenen, mithin nur zu dessen gespeicherten Aufzeichnungen bekannt werden, werden keine dem Dienstleistungsanbieter von weiteren Nutzern anvertraute Daten eingesehen. Daher wahrt es den Rechtsschutz des Anbieters, dass dieser nach § 110 Abs. 3 S. 2 Hs. 2 StPO durch die entsprechende Anwendung von § 98 Abs. 2 StPO bei einem Zugriff auf seine Daten eine richterliche Bestätigung der Beschlagnahme beantragen kann.[715] Im Zuge dieser binnen drei Tagen einzuholenden gerichtlichen Entscheidung, muss sodann auch dem Dienstleistungsanbieter nach § 33 Abs. 3 StPO rechtliches Gehör gewährt werden.[716] Im Übrigen schützt die Offenheit einer Maßnahme nur den unmittelbar durch sie Betroffenen, nicht jedoch inhaltlich Unbetroffene wie den Dienstleistungsanbieter.[717]

713 *Graf* in: BeckOK-StPO, § 100j StPO, Rn. 20, der davon ausgeht, dass die Möglichkeiten strafprozessualer Zugriffe auf Zugangsdaten durch die Neufassung des § 100j StPO nunmehr abschließend geregelt sind eine Umgehung der hierdurch festgeschriebenen Vorgehensweise und der damit einhergehenden Anforderungen rechtswidrig sein wird; ebenso *Burhoff*, StRR 2015, 8, 9.

714 *Gercke* in: HK-StPO, § 110 StPO, Rn. 34; *Singelnstein*, NStZ 2012, 593, 598.

715 *Bär*, ZIS 2011, 53, 54.

716 A.A.: *Puschke/Singelnstein*, NJW 2008, 113, 115.

717 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 375.

X) § 94 ff. StPO

1) Durchsuchung und Beschlagnahme beim Verdächtigen

Erfolgt sodann eine Durchsuchung beim Verdächtigen, im Zuge derer auch die genutzte Cloud durchsucht werden soll, stellt sich die Frage auf, welche Rechtsgrundlage diese Durchsuchung der Cloud zu stützen ist. Richtet sich die Durchsuchung der Cloud nach § 102 StPO könnte sie bei dem, der als Täter oder Teilnehmer einer Straftat verdächtig ist, bereits dann vorgenommen werden, wenn lediglich zu vermuten ist, dass die Durchsuchung zum Auffinden von Beweismitteln führen wird. Würde sich die Durchsuchung der Cloud dagegen nach § 103 StPO richten, wäre für deren Durchsuchung erforderlich, dass Tatsachen die Annahme begründen, die gesuchte Spur oder Sache befinde sich in den zu durchsuchenden Räumen, mithin in der Cloud. In diesem letztgenannten Fall wären die Anordnungsvoraussetzungen bedeutend strenger. Eine Durchsuchungsanordnung nach § 102 StPO sieht sich dabei vor allem dem Problem gegenüber, dass die zu durchsuchende Sache als dem Beschuldigten gehörend anzusehen sein müsste. Daher könnte anzunehmen sein, dass der Cloud-Speicher eine dem Beschuldigten gehörende Sache darstellen müsste. Dabei kommt es nicht auf die genaue Eigentumszuordnung an, vielmehr ist bereits der Besitz an einer solchen Sache ausreichend, um sie als dem Beschuldigten gehörend anzusehen.[718] Für einen Besitz ist in diesem Zusammenhang lediglich erforderlich, dass der Verdächtige wenigstens Mitgewahrsam in Form einer faktischen Zugriffsmöglichkeit auf die Daten besitzt.[719] Der Anwendbarkeit des § 102 StPO würde daher lediglich der Alleingewahrsam des Cloud-Anbieters entgegenstehen. Der Gewahrsam beschreibt ein tatsächliches Herrschaftsverhältnis über die Sache, das von einem Herrschaftswillen und der tatsächlichen Verfügungsgewalt getragen wird.[720] Zwar hat der Cloud-Nutzer keinen Zugriff auf den Cloud-Server als solchen und damit folgerichtig bereits unstreitig nicht einmal Mitgewahrsam an diesem. Angesichts dessen, dass aber nicht die Art des durchsuchten Mediums, sondern sein Inhalt (d.h. die Eignung der aufzufindenden Daten als Beweismittel) entscheidend für die Anordnung

718 BGH, StV 2007, 60, 61.
719 *Tsambikakis* in: LR-StPO, § 102 StPO, Rn. 40; *Wohlers/Jäger* in: SK-StPO, § 102 StPO, Rn. 15a; *Köhler* in: Meyer-Goßner/Schmitt, § 102 StPO, Rn. 10a.
720 *Kindhäuser* in: NK-StGB, § 242 StGB, Rn. 29 f.

der Durchsuchung ist,[721] muss entscheidender Bezugspunkt im Rahmen des § 102 StPO nicht der Gewahrsam des Betroffenen an dem Server als Datenträger, sondern an den hierauf abgespeicherten Inhaltsdaten sein.

Dies bestätigt auch ein Vergleich mit der Situation der E-Mail-Beschlagnahme. Auch dabei ist bezüglich der Gewahrsamszuordnung entscheidend, dass der Verdächtige faktische Zugriffmöglichkeiten auf die Nachrichten einschließlich der Datenanhänge hat. Es wird bei der Durchsuchung und Beschlagnahme im Falle von E-Mails daher nicht auf den Server als Sache abgestellt, sondern gefragt, ob der Nutzer eine Verfügungsmöglichkeit über die E-Mails – oder über die gespeicherten Daten in der Cloud – innehat.[722] Ebenso können für die Gewahrsamseinordnung in der Cloud die Grundsätze zu Durchsuchungen bei gemieteten Räumen herangezogen werden. Bei einer Durchsuchung in einem Hotelzimmer genügt ebenfalls eine Anordnung nach § 102 StPO, da aufgrund der vertraglich geregelten Nutzungsüberlassung eine Verfügungsbefugnis – und daher Gewahrsam – des Hotelzimmerbewohners besteht.[723] Bei Daten in der Cloud ist es deshalb sachgerecht, auf die Verfügungsgewalt hinsichtlich der gespeicherten Daten selbst und nicht hinsichtlich des Datenträgers – vergleichbar mit dem Hotelzimmer, in dem der Gast seine persönlichen Dinge ablegt – abzustellen.[724] Auch wenn der Cloud-Nutzer also keinen Gewahrsam an dem Datenträger als Sache hat, so hat er die erforderliche Verfügungsgewalt an dem in der Cloud gespeicherten Datenbestand. Ein solcher Mitgewahrsam kommt den Sprachassistenznutzern unter anderem entscheidend durch die vorhandene Löschungsmöglichkeit der aufgezeichneten Audio-Dateien zu. Es ist dem Kunden des Dienstleistungsanbieter jederzeit möglich durch ein Login die Tür zum persönlichen Cloud-Speicher zu öffnen und Aufzeichnungen zu löschen. Dieser Mitgewahrsam in Form des faktischen Zugriffs auf die Sache und ihren Inhalt ist ausreichend, um die Durchsuchung der Cloud des Betroffenen auf § 102 StPO stützen zu können.

721 BGH, StV 2007, 60, 61.
722 *Wicker*, DSRITB 2013, 981, 989.
723 *Wicker*, DSRITB 2013, 981, 989.
724 *Wicker*, DSRITB 2013, 981, 989.

a) Ermächtigungsgrundlage zur Beschlagnahme

Entscheidend ist schließlich die Frage auf, welcher strafprozessualen Grundlage die im Rahmen der Durchsuchung aufgefundenen beweisrelevanten Daten beschlagnahmt werden dürfen. Während für den ähnlich gelagerten Fall der E-Mailbeschlagnahme als mögliche Ermächtigungsgrundlagen sowohl § 100a StPO, als auch § 94 StPO sowie § 99 StPO in Betracht kommen[725], muss § 100a StPO in Bezug auf die auf Servern des Sprachassistenten gespeicherten Audioaufzeichnungen konsequenterweise erneut von vorn herein ausscheiden.[726] Wenn schon während des Übermittlungsvorganges keine Telekommunikation vorliegt, so kann diese erst recht nicht vorliegen, wenn die Daten nicht mehr in Bewegung sind, sondern auf dem Server ruhen.

aa) § 99 StPO

In seiner richtungsweisenden Entscheidung zur E-Mail Beschlagnahme hielt der BGH eine Postbeschlagnahme nach § 99 StPO für möglich: Die Beschlagnahme von auf dem Server des E-Mail Providers gespeicherten Nachrichten ist mit der Beschlagnahme anderer Mitteilungen, die sich zumindest vorübergehend bei einem Post- oder Telekommunikationsdiensteleister befinden, vergleichbar.[727] Auch ohne spezifische gesetzliche Regelung sei die E-Mail-Beschlagnahme daher unter den Voraussetzungen des § 99 StPO zulässig. Es ist aber zu bezweifeln, ob dies auch für den Fall der Beschlagnahme von gespeicherten Cloud-Aufzeichnungen gelten kann. Schließlich stützte der BGH die Anwendbarkeit des § 99 StPO entscheidend auf die Vergleichbarkeit der E-Mail-Kommunikation mit der postalischen Briefkommunikation, bei welcher sich der zu beschlagnahmende Brief zur Überbringung an die Zielperson im Gewahrsam des Postdienstleisters befinden müssen. Auf den der Nutzung eines Sprachassistenten zugrunde liegenden Sachverhalt ist dieser Vergleich jedoch nur eingeschränkt anwendbar. Zum einen handelt es sich bei den hier aufge-

725 Vgl. *Szebrowski*, MMR 2009, V, m.w.N.

726 A.A. hinsichtlich der Einschlägigkeit des § 100a StPO BGH, NJW 2021, 1252, 1554; im Ergebnis zustimmend *Abraham*, HRRS 2021, 356, 364 f.; kritisch vgl. *Grözinger*, NStZ 2021, 358 f.; *Hiéramente* WiJ 2021, 19, 21 f.; vgl. dazu im Übrigen oben Fn. 401.

727 BGH, NJW 2009, 1828, 1828.

zeichneten Daten bereits um keine an den Verdächtigen gerichtete Kommunikation. Zum anderen wurde der Inhalt der Audioaufzeichnungen auch gerade nicht zum Zwecke der Übermittlung in den Gewahrsam des Dienstleistungsanbieters gegeben. Der Inhalt der Aufzeichnungen wird von diesem vielmehr zur Verbesserung seines eigenen Angebots gespeichert. Hinsichtlich § 99 StPO muss ferner entscheidend sein, dass es sich bei den beschlagnahmten Gegenständen, um von diesen Unternehmen beförderte Sendungen handelt. Wenngleich der BGH unter den Sendungsbegriff in entsprechender Anwendung auch nicht-körperliche Nachrichten fasste, ist für eine solche Sendung stets typisch, dass die versendete Nachricht zur Kenntnisnahme an einen Menschen versandt wird[728] und anschließend an einer anderen Stelle inhaltsgleich in Empfang genommen wird. Bei der Nutzung eines Sprachassistenten wird anders als im Falle des E-Mail-Verkehrs die übermittelten Nachrichten nicht als solche an einer anderen Stelle abgeliefert, sondern lediglich die in der Nachricht enthaltene Anweisung ausgeführt. Vor allem geht es dabei nicht um die Übermittlung, um der Übermittlung willen, sondern es steht die Übermittlung zur Befehlsausführung im Vordergrund. Die im Rahmen der Nutzung eines Sprachassistenten aufgezeichneten Audiodaten können daher nicht als Sendung im Sinne von § 99 StPO erfasst werden. § 99 StPO stellt daher keine taugliche Ermächtigungsgrundlage dar.

bb) § 94 StPO

In Betracht kommt darüber hinaus die allgemeine Beschlagnahmevorschrift, § 94 StPO. Diese ist weiter gefasst als die Vorschrift der Postbeschlagnahme. Jedoch sind Daten keine körperlichen Gegenstände und so grundsätzlich kein taugliches Beschlagnahmeobjekt sein.[729] Da die zu beschlagnahmenden Informationen vorerst nicht in körperlichen Gegenständen manifestiert sind, würde grundsätzlich nur die Beschlagnahme der entsprechenden Hardware in Betracht kommen. Die Beschlagnahme einer kompletten EDV-Anlage dürfte jedoch in vielen Fällen, gerade sofern in Wirtschaftsstrafsachen dadurch ganze Unternehmen zum Erliegen kommen würden, unverhältnismäßig sein. Gleiches gilt für die Beschlagnahme

728 Vgl. *Menges* in: LR-StPO, § 99 StPO, Rn. 25.

729 *Wohlers* in: SK-StPO, § 94 StPO, Rn. 26; *Gercke* in: HK-StPO, § 94 Rn. 18; *Lemcke*, Die Sicherstellung, S. 19 ff.; *Bär*, MMR 1998, 577, 579; *Kemper*, NStZ 2005, 538, 541.

eines kompletten Servers, auf dem darüber hinaus auch eine Vielzahl an Informationen Dritter gespeichert sind. Durch die Beschlagnahme der EDV-Anlage oder des Servers würde zudem ein Eingriff in Art. 14 GG und vielfach auch in Art. 12 GG des Betroffenen erfolgen.[730] Daher wird in der Praxis die Anfertigung von Kopien der gangbare Weg zur Umsetzung der Beschlagnahme darstellen.[731]

Mangels hierfür vorhandener Ermächtigungsgrundlage und eines daraus folgenden Verstoßes gegen den Vorbehalt des Gesetzes könnte dies kritisch gesehen werden.[732] Da das Duplizieren der Aufzeichnungen oder Daten letztlich eine Maßnahme darstellt, die im Vergleich zu einer Beschlagnahme des Nutzerkontos oder gar des kompletten Servers die Eingriffsintensität verringert, muss das Ergebnis eines Erst-Recht-Schluss sein, dass nicht zuletzt die Verhältnismäßigkeit das Anfertigen bloßer Kopie der Daten in der Praxis – sofern ebenfalls unter verhältnismäßigem Aufwand möglich – gebietet.[733] Zum Umgang mit dieser Situation haben sich daher zwei Lösungsmöglichkeiten entwickelt. Entgegen dem vermeintlichen Wortlaut („Gegenstände") soll es auf die Körperlichkeit im Zusammenhang mit elektronischen Daten nicht ankommen. Denn für den historischen Gesetzgeber war im Zeitpunkt der Normschaffung nicht ersichtlich, dass elektronische Daten als nichtkörperliche Informationen für die Beweisführung im Strafverfahren noch bedeutsam werden könnten.[734] Im weiteren Verlauf zeigte jedoch die Ergänzung der Strafprozessordnung um die §§ 98a ff. StPO, dass der Gesetzgeber sodann auch von der Beschlagnahmefähigkeit von Datenbeständen ausgegangen ist.[735] § 94 StPO erfasst somit sämtliche Gegenstände, denen ein Beweiswert zukommen kann und die für die Untersuchung von Bedeutung sein könnten.[736] Ebenso wie das Anfertigen von Kopien im Falle der Beschlagnahme von körperlichen

730 *Menges* in: LR-StPO, § 94 StPO, Rn. 28 m.w.N.
731 *Süptitz/Utz/Eymann*, DuD 2013, 307, 309; *Menges* in: LR-StPO, § 94 StPO, Rn. 14; *Kassebohm* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 43, Rn. 434; *Basar/Hiéramente*, NStZ 2018, 681, 682.
732 Vgl. zur Problematik *Bell*, Beschlagnahme und Akteneinsicht, S. 99 ff.
733 *Köhler* in: Meyer-Goßner/Schmitt, § 94 StPO, Rn. 16b; *Kemper*, NStZ 2005, 538, 540.
734 BVerfGE 113, 29, 50.
735 BVerfGE 113, 29, 50.
736 Vgl. BGH, StV 2007, 60, 61; *Menges* in: LR-StPO, § 94 StPO, Rn. 11; *Gerhold* in: BeckOK-StPO, § 94 StPO, Rn. 3; *Köhler* in: Meyer-Goßner/Schmitt, § 94 StPO, Rn. 16b.

Unterlagen seit langem anerkannt ist[737], kann auch das Anfertigen von Kopien digitaler Daten ohne Weiteres auf § 94 StPO gestützt werden. Dieses Ergebnis stützt eine Literaturauffassung zudem darauf, dass in der Datenkopie ein Minus zur Beschlagnahme des Servers liegt, sodass eine Datenkopie nach § 94 StPO zulässig ist, obwohl unkörperliche Daten für sich nicht § 94 StPO unterliegen.[738]

Bereits hinsichtlich der Beschlagnahme von E-Mails wurde das Vorgehen nach § 94 StPO aufgrund eines Eingriffs in Art. 10 GG, der durch § 94 StPO nicht zu rechtfertigen sei, scharf kritisiert.[739] Im Zusammenhang mit der verfassungsrechtlichen Einordnung einer E-Mail wird gemeinhin zwischen dem Weg der E-Mail vom Absender bis zum Ankommen im Speicher des Serverbetreibers (Phase 1), der dortigen Speicherung vor der Kenntnisnahme (Phase 2), dem anschließenden Abruf durch den Empfänger (Phase 3) und der abschließende Speicherung der E-Mail im Online-Postfach des Providers (Phase 4) unterschieden.[740] Während die erste und dritte Phase nahezu einhellig dem Schutzbereich des Fernmeldegeheimnisses zugeordnet werden, ist die Zuordnung in den Phasen 2 und 4 deutlich umstrittener.[741] Korrekt ist jedoch, dass der Schutzbereich aus Art. 10 GG trotz der ruhenden Kommunikation (aufgrund der Speicherung der Nachrichten auf dem Server des Providers) auch in Phase 2 und 4 eröffnet ist.[742] Zwar kann der Nutzer durch Zugangssicherungen wie Passwörter versuchen, die auf dem Server gespeicherten Nachrichten vor einem Zugriff Dritter zu schützen. Er hat jedoch keine technische Möglichkeit, die Weitergabe der Nachrichten durch den Dienstleistungsanbieter – der gerade nicht Kommunikationsteilnehmer ist – zu verhindern. Dieser fortbestehende technisch bedingte Mangel an Beherrschbarkeit ist ausschlaggebend für den besonderen Schutz, der auch ruhenden Daten in den Phasen 2 und 4 durch das Fernmeldegeheimnis zuteilwer-

737 *Ciolek-Krepold*, Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, Rn. 358; *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, S. 275.

738 *Wohlers* in: SK-StPO, § 94 StPO, Rn. 26; *Gercke* in: HK-StPO, § 94 Rn. 18, 22; *Schäfer* wistra 1989, 8, 12; *Weber/Meckbach*, NStZ 2006, 492, 493.

739 *Beulke/Swoboda*, Strafprozessrecht, Rn. 392.

740 *Krüger*, MMR 2009 680, 681.

741 *Krüger*, MMR 2009 680, 681.

742 BVerfGE 124, 43, 55.; *Grözinger*, GA 2019, 441, 446; *Neuhöfer*, JR 2015, 21, 23; *Kleine-Vossbeck*, Electronic Mail, S. 142 f.; anders ist dies in den Fällen, in denen nach Abschluss eines Kommunikationsvorgangs gespeicherte Inhalte der zuvor durchgeführten Kommunikation im Herrschaftsbereich *eines* Kommunikationsteilnehmers ruhen, vgl. BVerfGE 124, 43, 54 f.; *Wenzel*, NZWiSt 2016, 85, 88.

den muss.[743] Aus der Eröffnung des Schutzbereiches wird sodann gefolgert, dass jedenfalls in Phase 2 ein Zugriff nur unter den strengeren Eingriffsvoraussetzungen des § 100a StPO möglich sei. Andernfalls würde der Schutz während dieses Stadiums aufgrund der technisch notwendigen Zwischenspeicherung auf dem Server des Providers abgeschwächt, da bereits unter den geringeren Eingriffsvoraussetzungen des § 94 StPO ein Zugriff erfolgen könnte.[744] Das BVerfG hält dem entgegen, dass sich weder aus der Systematik oder dem Telos der 94 ff. StPO noch den Gesetzesmaterialien Anhaltspunkte entnehmen lassen, dass ein Eingriff in Art. 10 GG nur aufgrund von § 99, § 100a und § 100g StPO zulässig ist.[745] Die Differenzierung in verschiedene zeitliche Stadien zugrunde legend, kommen im Falle eines staatlichen Zugriffs nach der Kenntnisnahme durch den Empfänger und dem Verbleiben der Nachricht auf dem Provider-Server (Phase 4) jedoch selbst die Kritiker der höchstrichterlichen Rechtsprechung zu dem Schluss, dass aufgrund der bewussten Entscheidung des Nutzers die Daten auf einem fremden Server zu speichern, ein Zugriff über § 94 StPO – trotz der durch das Bundesverfassungsgericht festgestellten Betroffenheit des Art. 10 GG, die unabhängig von einer Zwischen- oder Endspeicherung gegeben ist[746] – nicht zu beanstanden ist.[747]

Es ist jedoch bereits fraglich, ob die Diskussion hinsichtlich der Zugriffsmöglichkeiten in Phase 2 bei der Nutzung eines Sprachassistenten überhaupt zum Tragen kommt. Schließlich befinden sich die Daten zu keiner Zeit zum Abruf bereit auf dem Server des Dienstleistungsanbieters, sondern werden durch den Nutzer (im Sinne der E-Mail-Rechtsprechung des BGH daher durch den Absender) in die Cloud transportiert. Die Situation ähnelt daher weniger dem Stadium „Ruhen auf dem Serverprovider vor Abruf durch den Empfänger", sondern vielmehr dem Stadium „Verbleiben der Nachricht auf Server nach Kenntniserlangung (Phase 4)".[748] Schließlich besteht für die Benutzer des Sprachassistenten – jedenfalls in der Theorie – die Möglichkeit, Aufzeichnungen aus der

743 BVerfGE 124, 43, 55, vgl. zur Schutzbereichseröffnung auch § 4, B), I), 2), c); a.A.: *Krüger*, MMR 2009 680, 682; *Brunst*, CR 2009, 591, 592.

744 *Beulke/Swoboda*, Strafprozessrecht, Rn. 392; *Neuhöfer*, JR 2015, 21, 24; FS-Hamm/*Spatscheck*, 733,

747; *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 305; *Meinicke*, DSRITB 2012, 773, 784 f.

745 BVerfGE 124, 43, 58 f.

746 BVerfGE 124, 43, 55.

747 *Beulke/Swoboda*, Strafprozessrecht, Rn. 392.

748 Vgl. *Schelzke*, HRRS 2013, 86, 89.

Cloud zu löschen.[749] Dadurch würde den Nutzern zu einem gewissen Grad die Herrschaft über ihre Daten zurückübertragen. Verwaltet der Nutzer seine Daten anschließend nicht aktiv (indem er beispielsweise solche löscht), handelt es sich um eine bewusste Entscheidung des Nutzers seine Aufzeichnungen unter anderem zur Verbesserung des genutzten Systems in der Cloud zu belassen. Dies ist vergleichbar mit der Aufbewahrung einer Akte mit diversen Unterlagen, bei der sich der Betroffene ebenfalls bewusst dazu entscheidet, die darin verkörperten Inhalte nicht zu vernichten. Deren Beschlagnahme erfolgt klassischerweise auf Grundlage des § 94 StPO. Insofern ist es nur folgerichtig auch die auf einer Cloud gespeicherten Daten über § 94 StPO zu beschlagnahmen.[750]

2) Durchsuchung und Beschlagnahme beim Dienstleistungsanbieter

Verlief die Durchsuchung beim Verdächtigen nach § 102 StPO nicht erfolgreich, sodass die Beamten auch keine Daten nach § 110 Abs. 3 StPO sichten konnten, da es beispielsweise nicht gelang die Passwörter zum Accountlogin ausfindig zu machen, wird die Möglichkeit der Durchsuchung und der Beschlagnahme beim Dienstleistungsanbieter relevant. In diesen Fällen müssen die zielführenden Maßnahmen gegenüber demjenigen ergriffen werden, der die Daten in unmittelbarem Gewahrsam hat. Als Gewahrsamsinhaber kennzeichnet sich derjenige, der unmittelbaren Zugriff auf das externe Speichermedium hat,[751] mithin jedenfalls der Dienstleistungsanbieter und Inhaber der Serversysteme. Gem. § 103 StPO ist die Durchsuchung auch bei „anderen Personen" möglich. Als andere Person im Sinne des § 103 StPO werden alle Personen erfasst, die im Zusammenhang mit der Durchsuchung zugrunde liegenden Strafverfahren nicht als Beschuldigte gelten.[752] Auf den betroffenen Serversystemen sind darüber hinaus weitere Daten von einer Vielzahl gänzlich unbeteiligter Personen gespeichert. Daher gewinnt im Zusammenhang mit der Durchsuchung beim Dienstleistungsanbieter auch § 108 StPO an Bedeutung. § 108 StPO erlaubt den Strafverfolgungsbehörden, Aufzeichnungen die im Rahmen

749 Vgl. https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (abgerufen am 31.10.2021).
750 Vgl. im Ergebnis *Dalby*, CR 2013, 361, 368; *Gless*, StV 2018, 671, 673; *Anders*, ZIS 2020, 70, 75; a.A.: *Neuhöfer*, JR 2015, 21, 25 f.
751 *Obenhaus*, NJW 2010, 651, 653.
752 *Köhler* in: Meyer-Goßner/Schmitt, § 103 StPO, Rn. 1.

der Durchsuchung entdeckt werden und auf eine andere, durch die mit der Anordnung der Durchsuchung nicht in Verbindung stehende Straftat hindeuten, zu beschlagnahmen. Diese „Gefahr" für sämtliche durch eine Serverdurchsuchung beim Dienstleistungsanbieter mittelbar betroffenen Kunden, wird durch die heutige Technik größtenteils entschärft, da eine saubere Trennung der Daten der einzelnen Nutzer auf dem durchsuchten Server gewährleistet ist. Sämtliche Daten können dem betreffenden Nutzer zugeordnet werden, sodass die Behörden bei einer Durchsuchung nur den dem Beschuldigten zugeordneten Datensatz durchsuchen. Eine wirkliche Suche, bei der auch den Dienstleistungsanbieter selbst oder dessen weitere Kunden belastendes Material gefunden werden könnte, findet folglich gar nicht statt. Daher ist die Gefahr hinsichtlich eines Zufallsfundes nach § 108 StPO sehr gering.[753] Aufgrund dieser technischen Separationsmöglichkeit und dem Ausschluss der Gefahr für Dritte stellt sich jedoch erneut die Frage, ob es sich sodann überhaupt um eine Durchsuchung gem. § 103 StPO oder nicht vielmehr um eine solche beim Verdächtigen, die auch nach § 102 StPO durchgeführt werden kann, handelt.

Dabei sind zwei Situationen zu unterscheiden. Zum einen könnte der Dienstleistungsanbieter seiner Verpflichtung aus § 95 StPO folgend den entsprechenden Datensatz freiwillig herausgeben. In dieser Situation vergleicht *Bell* die Durchsuchung beim Dienstleistungsanbieters mit der Durchsuchung eines Bankschließfaches, da die Beamten dort wie auch bei der Durchsuchung der Cloud lediglich die Sachen bzw. Daten des Verdächtigen, nicht jedoch auch fremde Räume wie die des Dienstleistungsanbieters, durchsuchen.[754] Dem ist zuzustimmen, denn die Suche nach beweisrelevanten Daten findet auch bei der Durchsuchung eines Cloudnetzwerkes erst innerhalb des dem Verdächtigen zugeordneten Datensatzes und nicht innerhalb der kompletten Cloud statt.[755] Weigert sich der Dienstleistungsanbieter jedoch die Daten des Beschuldigten Cloud-Nutzers herauszugeben, ist eine umfassende Durchsuchung auf dessen Cloud-Servern notwendig. Da sodann der komplette Datenträger des Dienstleistungsanbieters durchsucht wird, muss sich diese Durchsuchung auch deshalb nach dem strengeren § 103 StPO richten.[756]

---

753 *Bell*, Strafverfolgung und die Cloud, S. 131.

754 *Bell*, Strafverfolgung und die Cloud, S. 131; Wicker, Cloud-Computing und staatlicher Strafanspruch, S. 349 f.

755 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 348.

756 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 350, dies. DSRITB 2013, 981, 991.

Teilweise wird dagegen eingewandt, dass unter Heranziehung des § 103 Abs. 2 StPO auch eine solche Durchsuchung beim Dienstleistungsanbieter nach den Voraussetzungen des § 102 StPO ablaufen könne.[757] Nach § 103 Abs. 2 StPO gelten die strengeren Beschränkungen des § 103 Abs. 1 StPO nicht für Räume, deren Inhaber zwar ein Dritter ist, in denen sich jedoch der Beschuldigte im Zusammenhang mit der Verfolgung aufgehalten hat. Bezogen auf eine Cloud sei es erforderlich, den Gehalt des § 103 Abs. 2 StPO, der von der körperlichen Anwesenheit des Verdächtigen ausgeht, so anzuwenden, dass der verdächtige Cloud-Nutzer sich bei der Nutzung des Speicherdienstes dort aufgehalten hat, wenngleich er dort nicht körperlich anwesend war. Hierfür spreche der Technikfortschritt, der es erfordere, nicht auf die faktische körperliche Anwesenheit des Verdächtigen abzustellen, sondern auch einen virtuellen Zugang genügen zu lassen.[758] Diese Sichtweise würde jedoch den eigentlichen Inhalt des § 103 Abs. 2 StPO überstrapazieren. Dieser lässt eine Anordnung nach §§ 102, 103 Abs. 2 StPO unter den Voraussetzungen des § 102 StPO nur zu, wenn der Beschuldigte in den durchsuchten Räumen ergriffen wird oder sich dort während seiner Verfolgung aufgehalten hat. Insofern fordert § 103 Abs. 2 StPO ein Aufhalten in einem solchen Raum während seiner Flucht und nicht zu einem beliebigen in der Vergangenheit liegenden Zeitpunkt.[759] Wenn jede Cloudnutzung als Aufenthalt im Sinne des § 103 Abs. 2 StPO eingeordnet wird, wird damit die weitere Voraussetzung, dass sich der Betroffene während dieses Aufenthalts zusätzlich auf der Flucht befunden haben muss, übergangen. Es müsste daher für eine Durchsuchung beim Dienstleistungsanbieter gem. §§ 102, 103 Abs. 2 StPO feststehen, dass der Betroffene sich während der Speicherung der Audioaufzeichnungen bereits auf der Flucht befand.

Hinsichtlich des praktischen Ablaufs einer Beschlagnahme beim Dienstleistungsanbieter wird befürchtet, dass die hierfür zuständigen Kontaktstellen des Unternehmers den Behörden freiwillig über die gesetzliche Verpflichtung hinausgehende Unterstützungsleistungen anbieten und so der Schutz des Verdächtigen, dem in gewisser Weise sämtliche Ermittlungsbefugnisse mittelbar dienen, untergraben wird.[760] Diese für den Verdächtigen missliche Situation ist jedoch aus strafprozessualer Sicht jedenfalls auf

757 *Wicker*, DSRITB 2013, 981, 992 f.
758 *Wicker*, DSRITB 2013, 981, 993.
759 *Hegmann* in: BeckOK-StPO, § 103 StPO, Rn. 19; *Hauschild* in: MüKo-StPO, § 103 StPO, Rn. 14.
760 *Gercke* in: Borges/Meents Cloud-Computing, § 20, Rn. 38.

Ebene des bloßen Zugriffs auf etwaige Daten nicht zu beanstanden. Zwischen dem betroffenen Nutzer und dem Dienstleistungsanbieter besteht kein besonderes Vertrauensverhältnis auf Grund dessen zu befürchten wäre, dass sich dieser mit der Preisgabe etwaiger Informationen zurückhalten würde. Die Ermittlungsbehörden sind jedoch als an Recht und Gesetz gebundenen Teile der Exekutive angehalten, den Zeitraum, aus welchem Unterlagen benötigt werden, möglichst genau einzugrenzen, sodass die Dienstleistungsanbieter nicht aus vermeintlichem Selbstschutz sämtliche gespeicherte Daten über den betroffenen Nutzer offenlegen.[761]

3) Ergebnis

Bestehen Anhaltspunkte, dass ein Sprachassistent belastende Aufzeichnungen aufgezeichnet haben könnte und diese in der Cloud des Dienstleistungsanbieters gespeichert sind, besteht zunächst die Möglichkeit im Rahmen einer Durchsuchung beim Verdächtigen, § 102 StPO, sich in dessen Account einzuloggen und eine Sichtung der dort aufgezeichneten Audio-Dateien vorzunehmen, § 110 Abs. 3 StPO. Sodann kann zur genaueren Überprüfung eine Sicherungskopie erstellt werden, um die entsprechenden Aufzeichnungen in den Räumen der Strafverfolgungsbehörden auszuwerten. Ergeben sich keine beweisrelevanten Informationen sind die Sicherungskopien unverzüglich zu löschen und der Betroffene zu benachrichtigen, andernfalls sind die Unterlagen durch richterlichen Beschluss zu beschlagnahmen.[762] Ein mehrmaliges Einloggen in den Account des Betroffenen zu einer fortlaufenden Sichtung der dort gespeicherten Aufzeichnungen ist nicht von der Befugnisnorm umfasst. Dem Betroffen wird dennoch zu raten sein, sein Passwort zu ändern. Zudem können die Strafverfolgungsbehörden auch eine offene Durchsuchung des Serveraccounts beim Dienstleistungsanbieter vornehmen, die sich ebenfalls nach § 102 StPO richtet. Werden im Rahmen einer Durchsuchung belastende Aufzeichnungen entdeckt, können auch solche digital in einer Cloud gespeicherte Daten gem. § 94 StPO, beschlagnahmt werden. Dies kann wiederum sowohl beim Verdächtigen, sofern das Passwort zum Zugang in die Cloud ausfindig gemacht werden kann, als auch beim Dienstleistungsanbieter vor Ort geschehen. Im zweiten Fall wird es jedoch regelmäßig als Minusmaßnahme genügen, eine Kopie der Datenbestände zu fertigen, um

761 *Wicker*, Cloud-Computing und staatlicher Strafanspruch, S. 374.
762 *Wohlers/Jäger* in: SK-StPO, § 110 StPO, Rn. 27.

nicht komplette Server durch eine staatliche Beschlagnahme zum Erliegen zu bringen.

XI) Ermittlungsgeneralklausel, § 161 StPO

Bei einer entsprechend geringeren Grundrechtsrelevanz kommt als Ermächtigungsgrundlage auch die Ermittlungsgeneralklausel des § 161 Abs. 1 StPO in Betracht. Diese ermächtigt die Ermittlungsbehörden zum Zugriff auf alle öffentlich zugänglichen Informationen.[763] Bezüglich elektronischer Beweismittel ist im Zusammenhang mit der Generalklausel oft von einer Beweisbeschaffung durch eine „virtuelle Streife"[764] zu lesen. Dabei werden frei zugängliche Informationen wie Chatrooms oder Websites durch die Ermittlungsbehörden auf strafbare Handlungen überprüft.[765] Der freie Zugang für jedermann hat zur Folge, dass grundsätzlich kein Eingriff in die Grundrechte des Betroffenen vorliegt.[766] Dies liegt darin begründet, dass, infolge des freien Zugangs kein Vertrauen in die Identität und Diskretion der Kommunikationspartner bestehen kann. Dem Internetnutzer muss insofern bekannt sein, dass er die Angaben seines Gesprächspartners nicht überprüfen kann und sodann die sich hieraus ergebenden Kommunikationsbeziehungen nicht schutzwürdig sein können.[767] Der Nutzer geht vielmehr bewusst das Risiko ein, dass es sich bei seiner Gesprächsperson auch um staatliche Ermittlungsbeamte handeln könnte oder diese einen Chatverlauf in öffentlichen Foren mitlesen können.

Die Position des BVerfG ist an dieser Stelle jedoch nicht unumstritten. So werden Bedenken laut, dass nur auf Grundlage einer leichter vorzunehmenden Täuschung im Internetverkehr und der deswegen fehlenden Schutzwürdigkeit keine Generalerlaubnis für die Ermittlungsbehörden zur Ermittlung in offenen Bereichen des World Wide Web erfolgen dürfe.[768] Dabei wird sich eines Umkehrschlusses bedient, dass der digital Handelnde gerade aufgrund der geringeren Möglichkeiten die Identität des Kommunikationspartner im Internet zu ermitteln eine stärkere Absicherung

763 *Brunst* in: Gercke/Brunst, Internetstrafrecht, Rn. 782.
764 Vgl. dazu *Eisenmenger*, Die Grundrechtsrelevanz virtueller Streifenfahrten, S. 21 ff.
765 *Bär* in: Handbuch des Wirtschafts- und Steuerstrafrechts, Kapitel 28, Rn. 121.
766 BVerfGE 120, 274, 344 f.; *Hornick*, StraFo 2008, 281, 285.
767 BVerfGE 120, 274, 345.
768 *Eifert*, NVwZ 2008, 521, 522.

bedarf, als er dies in der nicht digitalen Welt bedürfte.[769] Diese Sichtweise verkennt jedoch, dass es gerade die Verantwortung des Einzelnen ist, wem er sich offenbart. Es ist nicht der Staat, der für eine stärke Absicherung des Einzelnen in Diskussionsforen oder Chatrooms Sorge tragen muss, sondern der verfassungsrechtlich gewollte mündige Bürger, der für sich selbst und die von ihm preisgegebenen Informationen in diesem Zusammenhang die uneingeschränkte Verantwortung trägt. Schließlich könnten die betroffenen Personen auch keinen Schutz ersuchen, wenn sie online nicht mit Beamten der Strafverfolgungsbehörden, sondern mit einem privaten Dritten kommunizieren und schließlich dieser sein erlangtes Wissen den Strafverfolgungsbehörden zur Verfügung stellt.[770]

Die Grenze eines Handelns auf Grundlage der Generalklausel wird aber dort zu ziehen sein, wo Informationen gezielt zusammengetragen, gespeichert und ausgewertet werden sollen.[771] Hier greift aufgrund einer Gefährdungslage für die Grundrechte des Einzelnen wieder der Gesetzesvorbehalt. Sofern beispielsweise der Zugang zu Foren, Chats oder ähnlichen nur nach einer Anmeldung mit echten Daten und einer Prüfung durch den Anbieter möglich ist, wäre der Staat beispielsweise darauf zu verweisen, verdeckte Ermittler unter einer Legende zu lassen – dies freilich nur bei Vorliegen der Voraussetzungen der speziellen Ermächtigungsgrundlage des § 110a StPO.[772] Auf die Generalklausel kann eine polizeiliche Streifenfahrt durch das Internet daher nur dann gestützt werden, wenn dabei Informationen gewonnen werden, die der Betroffene für die Öffentlichkeit frei zugänglich gemacht hat. Es dürfen daher keine Barrieren zu überwinden sein, um an die Informationen zu gelangen. Die Informationsbeschaffung müsste für jedermann auf gleiche Art ohne weitere Zwischenschritte möglich sein. Beispiele hierfür sind Beiträge in frei zugänglichen Foren. Bei der Nutzung eines Sprachassistenten begibt sich der Betroffene jedoch nicht in einen frei zugänglichen Bereich. Sofern dieser zur Informationsbeschaffung genutzt wird, erfolgt dieser Vorgang lediglich zwischen den Nutzer und den Severn des Dienstleistungsanbietern. Einen Dritten ist der Zugriff hierauf nicht ohne weiteres möglich. Zum Zugriff auf Sprachassistenten eignet sich die Ermittlungsgeneralklausel daher nicht.

769 *Brunst* in: Gercke/Brunst, Internetstrafrecht, Rn. 788.
770 So zur Hörfalle *Beulke/Swoboda*, Strafprozessrecht, Rn. 738, 742.
771 BVerfGE 120, 274, 345.
772 vgl. *Kudlich*, GA 2011, 193, 199.

XII) Übergeordnete Problematik: Serverstandort

Ein weiteres Problem in der praktischen Anwendung der Ermittlungsbefugnisse, die unmittelbar auf den Server des Dienstleistungsanbieters zugreifen, liegt darin begründet, dass die großen Anbieter von Cloud-Severn wie Apple, Google, oder Amazon mit ihrem Sitz nicht in Deutschland, sondern im Ausland angesiedelt sind. Daher stellt sich die Frage, inwiefern deutsches Strafprozessrecht zu Anwendung kommen kann. Ein Zugriff deutscher Behörden auf Server, die sich im Ausland befinden, würde ein Eingriff in fremde Souveränitätsrechte darstellen und setzt daher grundsätzlich ein Rechtshilfeersuchen an den betreffenden ausländischen Staat voraus.[773] Auch Ausnahmen von diesem Grundsatz, wie sie Art. 32 lit.a der Cybercrime Konvention normiert, werden in einem solchen Fall in der Regel nicht einschlägig sein. Weder sind die auf den Servern gespeicherten Daten öffentlich zugängliche Computerdaten, Art. 32 lit.a Cybercrime-Konvention, noch wird von einer freiwilligen Zustimmung der befugten Person zur Weitergabe der Daten an inländische Strafverfolgungsbehörden (Art. 32 lit. b Cybercrime-Konvention) ausgegangen werden können. Die inländischen Strafverfolgungsbehörden sind zur Durchführung eines Zugriffs sodann auf ein förmliches Rechtshilfeersuchen angewiesen. Sofern der Speicherort jedoch nicht feststellbar ist (was angesichts des Umstandes das international tätige Cloudanbieter die Rahmendaten der Datenspeicherung nicht immer offen legen werden nicht selten der Fall sein wird[774]) wird vertreten, dass in diesen Fällen auch ein Speicherort im Inland nicht ausgeschlossen werden kann.[775] Hierfür spreche, dass international agierende Anbieter für ihre Dienste in der Regel auch Host-Server in Deutschland benutzen. So wirbt beispielsweise Microsoft seit den Datenzugriffen US-amerikanischer Nachrichtendienste[776] damit, die Nutzerdaten unter Einhaltung des deutschen Datenschutzrechts in Deutschland zu speichern.[777] Da somit nicht jeder Zugriff auf Server eines ausländischen Unternehmens zwangsläufig zu einem tatsächlichen Zugriff auf im Ausland gespeicherte Daten führt, sollen entsprechende Maßnahmen nur

773 *Zerbes/El-Ghazi*, NStZ 2015, 425, 430; *Brunst*, DuD 2011, 618, 620 f.
774 *Bruns* in: KK-StPO, § 110 StPO, Rn. 8a; *Krause*, Kriminalistik 2014, 213, 215.
775 *Krause*, Kriminalistik 2014, 213, 215; *Soiné* NStZ 2018, 497, 500; *Angerer*, DRiZ 2019, 428, 431; *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 7b; *Wicker*, MMR 2013, 765, 768.
776 *Voigt*, MMR 2014, 158, 160.
777 Vgl. https://www.microsoft.com/de-de/cloud/deutsche-rechenzentren (zuletzt abgerufen am 31.10.2021).

unzulässig sein, wenn ein ausschließlich ausländischer Speicherort sicher feststeht.[778] Jedenfalls bei einer Maßnahme nach § 110 Abs. 3 StPO ist zudem zu beachten, dass sofern der Zugriff auf den Serveraccount über den Computer des Betroffenen erfolgt, es sich dabei um eine Ermittlungshandlung im Inland handelt, für die ohnehin kein Rechtshilfeersuchen zu stellen wäre.[779]

XII) Ergebnis

Der stetig wachsende Markt smarter Assistenten, bringt auch neue Ermittlungsmöglichkeiten für die Strafverfolgungsbehörden mit sich. Umsetzbar sind diese neuen Möglichkeiten nur unter strenger Beachtung des Gesetzesvorbehalts. Als möglicher Vorbehalt kann dabei jedenfalls § 100a StPO nicht dienen. Ein Zugriff auf Übermittlungsvorgänge zwischen Endgerät und Sprachassistent nach § 100a Abs. 1 S. 1, 2 StPO scheidet mangels des Vorliegens von Telekommunikation im Sinne des § 100a StPO ebenso aus, wie ein Zugriff auf ruhende, gespeicherte Telekommunikationsdaten nach § 100a Abs. 1 S. 3 StPO aufgrund der Verfassungswidrigkeit dieser Vorschrift. Auch die klassische Online-Durchsuchung nach § 100b StPO ist hinsichtlich des beim Betroffenen platzierten Endgeräts rechtlich zwar möglich, im Hinblick auf fehlende gespeicherte Datenbestände auf diesen Endgeräten in der Praxis jedoch nicht zielführend. Zielführender erscheint die ebenfalls unter § 100b StPO mögliche Live-Überwachung. Zwar dürfen sensorische Systeme des Smart Speakers dabei nicht bewusst aktiviert werden, allerdings ist es möglich, in Echtzeit ablaufende Geschehen in der Wohnung mitzuhören, sofern der Betroffene den Smart Speaker aktiviert. Umfangreichere Befugnisse bringt die Wohnraumüberwachung, die es erlaubt das Endgerät derart zu manipulieren, dass es als Wanze der Strafverfolgungsbehörden fungiert. Dann ist eine durchgehende akustische Wohnraumüberwachung des Betroffenen möglich, die nicht an die Aktivierung des Smart Speakers durch den Nutzer geknüpft ist. Auch wenn auf den Endgeräten ohnehin keine ruhenden Daten gespeichert sind, ist dafür Sorge zu tragen, dass die Software zur Manipulation des Sprachassistenten in Form des Smart Speakers derart konfiguriert ist, dass lediglich laufenden Kommunikationsvorgänge überwacht werden können.

---

778 *Bruns* in: KK-StPO, § 110 StPO, Rn. 8a.

779 *Wicker*, MMR 2013, 765, 769; *Köhler* in: Meyer-Goßner/Schmitt, § 110 StPO, Rn. 7b.

Hinsichtlich der offenen Ermittlungsbefugnissen ist zunächst auf eine Durchsuchung beim Verdächtigen, § 102 StPO zu verweisen. Im Rahmen derer sind die Strafverfolgungsbehörden ermächtigt mittels eines Keyloggers sich in Kenntnis der Zugangsdaten zum Account des Betroffenen zu bringen, um dort gespeicherte Daten sichten zu können, § 110 Abs. 3 StPO. Eine Bestandsdatenauskunft nach § 100j StPO ist zur Erlangung der Zugangsdaten aufgrund der Personenverschiedenheit von Access-Provider und Cloud-Anbieter nicht zielführend. Daneben kommt ebenso eine Durchsuchung des Serveraccounts beim Dienstleistungsanbieter nach § 102 StPO in Betracht. Eine Beschlagnahme im Rahmen der Durchsuchung aufgefundener beweisrelevanter Daten ist gem. § 94 StPO sowohl beim Verdächtigen als auch beim Dienstleistungsanbieter möglich. Es bestehen damit durchaus Möglichkeiten für die Strafverfolgungsbehörden unter Einhaltung des Gesetzesvorbehalts in bestimmten Situationen rechtmäßiger Weise auf Smart Speaker zu Ermittlungszwecken zuzugreifen.

§ 5 Verwertbarkeit

Nach einem erfolgten Datenzugriff ist in einem zweiten Schritt zu fragen, ob diese im Strafprozess zur Urteilsfindung als Beweis herangezogen werden können. Dies kann aus verschiedensten Gründen problematisch sein. Möglicherweise wurde bereits während des staatlichen Zugriffs gegen Rechtsvorschriften verstoßen, sodass die Beweismittel nicht vollständig rechtmäßig erlangt wurden. Ebenso ist es möglich, dass die Strafverfolgungsbehörden nicht durch einen eigens durchgeführten Zugriff in den Besitz entsprechender Informationen gelangt sind, sondern sie die Informationen von Privatpersonen übermittelt bekommen haben. Sodann kann für die Frage nach der Verwertbarkeit nicht außer Acht bleiben, wie diese Personen an die relevanten Informationen gelangt ist. Auch bei ordnungsgemäßer Beweiserhebung können beispielsweise verfassungsrechtliche Gründe gegen eine Verwertbarkeit der erlangten Informationen sprechen. Rund um die Frage der Existenz eines Beweisverbotes tritt erneut der Grundsatz, dass es keine Wahrheitsfindung um jeden Preis geben dürfe, in den Vordergrund. Der grundsätzliche geltende Untersuchungsgrundsatz aus § 244 Abs. 2 StPO und die freie richterliche Beweiswürdigung dürfen zur Wahrung eines rechtsstaatlichen Verfahrens nicht ohne Beachtung der Interessen und Rechte des Betroffenen durchgesetzt werden.[780]

A. Beweiserhebungsverbote

Bereits vor dem eigentlichen Prozess der Verwertung können im Rahmen der Beweisbeschaffung Verstöße gegen die Art und Weise der Beweisgewinnung, eine Beweisgewinnung über bestimmte Tatsachen oder eine Beweisgewinnung mittels bestimmter Mittel oder Methoden ein Beweisverbot nach sich ziehen. In diesen Fällen wird daher an den Akt der Beweiserhebung angeknüpft, der in der stattgefundenen Art und Weise hätte unterbleiben müssen. Im Rahmen möglicher Beweiserhebungsverbote wird regelmäßig zwischen Beweisthemaverbote, Beweismittelverbo-

780 *Beulke/Swoboda*, Strafprozessrecht, Rn. 51; vgl. im Übrigen die Ausführungen in § 3.

te und Beweismethodenverbote unterschieden.[781] Ein Beweisthemaverbot kann dann vorliegen, wenn über Tatsachen Beweis erhoben wurde, die nicht zum Gegenstand einer späteren Beweisführung gemacht werden dürfen.[782] Beispielhaft hierfür ist die Aufzeichnung von Gesprächen, die dem absolut geschützten Kernbereich zuzuordnen sind, vgl. § 100d Abs. 4 S. 2 StPO. Von Beweismittelverboten wird gemeinhin gesprochen, wenn das Beweisstück als Beweismittel im Strafverfahren ausgeschlossen ist. Dies gilt exemplarisch für zeugnisverweigerungsberechtigte Personen nach den §§ 52–55 StPO oder die Untersuchung respektive Blutabnahme bei Personen, die wiederum selbst berechtigt wären das Zeugnis zu verweigern, § 81c Abs. 3 StPO.[783] Unter ein Beweismethodenverbot fällt die Anwendung bestimmter verbotener Methoden zur Beweisgewinnung.[784] Hier ist insbesondere § 136a StPO zu nennen, der es verbietet, die Willensentschließung und Willensbetätigung des Verdächtigen durch die dort aufgezählten Methoden zu beeinträchtigen. Diese dreiteilige Differenzierung ermöglicht zwar eine systematische Unterteilung, kann aber keinen praktischen Mehrwert liefern. Wird trotz eines solchen Beweiserhebungsverbot der Beweis erhoben, so ist stets fraglich, ob hieraus auch ein Beweisverwertungsverbot entsteht.[785] Aus einem Beweiserhebungsverbot muss sich daher zunächst ein Beweisverwertungsverbot entwickeln, um von der Unverwertbarkeit des entsprechenden Beweismittels und mithin von einem Beweisverbot auszugehen.[786] Zu klären ist, inwiefern diese Punkte bei der Nutzung eines Sprachassistenten von Relevanz sein könnten.

I) Beweisthemaverbot

Von großer Bedeutung im Zusammenhang mit der Überwachung mittels eines Smart Speakers ist das den absoluten Kernbereich schützende Beweiserhebungsverbot des § 100d Abs. 4 S. 2 StPO bezüglich Maßnahmen nach § 100c StPO. Danach dürfen Maßnahmen nur dann angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Le-

781 *Kudlich* in: MüKo-StPO, Einl., Rn. 440.
782 *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 15; *Volk/Engländer,* GK StPO, § 28, Rn. 1.
783 *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 17.
784 *Eisenberg*, Beweisrecht der StPO, Rn. 347.
785 *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 21.
786 *Schmitt* in: Meyer-Goßner/Schmitt, Einl., Rn. 55.

bensgestaltung zuzurechnen sind, nicht erfasst werden. Der Kernbereichsschutz umfasst nicht nur den Schutz einzelner bestimmter Äußerungen, die wegen ihres Inhalts zum Schutz der Menschenwürde staatlicher Kenntnisnahme entzogen sein müssen, sondern zielt auf einen generellen Schutz der privaten Persönlichkeitsentfaltung ab. Zur praktischen Aufrechterhaltung der Menschenwürde muss es einen Bereich geben, der frei von jedweder staatlichen Kenntnisnahme bleibt.[787] Das anordnende Gericht muss sich daher die Frage stellen, ob eine gewisse Wahrscheinlichkeit dafür besteht, dass es zu einem Eingriff in den Kernbereich kommen würde und daher ein Beweiserhebungsverbot besteht.[788] Hierzu müssten tatsächliche Anhaltspunkte gegeben sein, aus denen jedenfalls typischerweise geschlossen werden kann, dass die abgehörte Kommunikation nicht den höchstpersönlichen Bereich betrifft.[789] Problematisch ist dabei vielfach, dass diese Entscheidung erst nach der Erhebung der Daten und der Kenntnis des Inhalts getroffen werden kann. Bereits durch die staatliche Kenntnisnahme wird der Kernbereich jedoch gewissermaßen tangiert.[790] Daher muss eine vor der Kommunikationserhebung durchzuführende negative Kernbereichsprognose ergeben, dass das zu erwartende Gespräch nicht dem Kernbereich zuzuordnen ist.[791] Um diese Einordung zu ermöglichen kann durch Vorermittlungen gesichert werden, dass die Maßnahme auf verfahrensrelevante Vorgänge begrenzt bleibt.[792]

Anders als bei der akustischen Wohnraumüberwachung für die § 100d Abs. 4 StPO neben dem Erfordernis einer negativen Kernbereichsprognose auch eine Abbruchpflicht bei der Gefahr einer akuten Kernbereichsverletzung beinhaltet, ist für die §§ 100a und 100b StPO keine vergleichbare Echtzeitüberwachung vorgesehen.[793] Kernbereichsverletzungen werden somit vielfach unvermeidbare Folgen einer solchen größtenteils automatisierten Überwachungsform.[794] Diese „Schutzlücke" kann im weiteren Ermittlungsverlauf erst auf Ebene der Beweisverwertung geschlossen werden. Insofern normiert § 100d Abs. 2 S. 1 StPO ein Beweisverwertungsverbot für alle nach § 100a StPO bis § 100c StPO erlangten Informationen, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind.

787 *Hoffmann-Riem*, JZ 2008, 1009, 1020.
788 *Bruns* in: KK-StPO, § 100d StPO, Rn. 11.
789 BVerfGE 109, 279, 320.
790 *Kutscha*, NJW 2007, 1169, 1171; *Hoffmann-Riem*, JZ 2008, 1009, 1020.
791 BVerfGE 109, 279, 320 f.
792 *Bruns* in: KK-StPO, StPO § 100d StPO, Rn. 12.
793 *Großmann*, JA 2019, 241, 246.
794 *Eschelbach* in: SSW-StPO, § 100d StPO, Rn. 16, 24.

1) Der Kernbereichsschutz auf Erhebungsebene

a) Entwicklung des Kernbereichsschutzes

Der Kernbereich nahm seinen Ursprung im Elfes-Urteil[795] des Bundesverfassungsgerichts aus dem Jahre 1957. Bis dato fiel die Entscheidung bei theoretisch kernbereichsrelevanten Inhalten stets im Wege einer Abwägung zwischen Individualschutz und Gemeinwohlinteresse nach Maßgabe des Verhältnismäßigkeitsgrundsatzes für oder gegen den Betroffenen. Mit der dem Elfes-Urteil zugrunde liegenden Verfassungsbeschwerde hatte erstmals eine solche deshalb Erfolg, weil das Gericht einen Eingriff in diesen unantastbaren, absolut geschützten Bereich bejahte.[796] In der die Rechtsprechung der kommenden Jahrzehnte prägenden Entscheidung, stellte das Gericht fest, dass sich aus der Menschenwürde eine dem Bürger zuzugestehende Sphäre privater Lebensgestaltung als unantastbarer Bereich menschlicher Freiheit ergeben müsse, die der Einwirkung öffentlicher Gewalt vollständig entzogen ist.[797] Während der Kernbereich in der Elfes-Entscheidung noch als „forum internum" verstanden wurde, das nur solche Vorgänge umfasse, die keinen Akt der Kommunikation darstellen, sondern lediglich Teil der Auseinandersetzung mit sich selbst waren[798], stellte das Bundesverfassungsgericht sodann im Tonbandaufnahme-Beschluss fest, dass auch kommunikative Sachverhalte zum Kernbereich der privaten Lebensgestaltung gehören können.[799] Im Zuge der zweiten Tagebuchentscheidung erhielten schließlich auch solche Vorgänge Zugang zum Kernbereich, die einen Sozialbezug zu Dritten aufweisen, da sich die menschliche Persönlichkeit notwendigerweise im Zusammenspiel mit sozialen Bezügen verwirkliche.[800] Das Bundesverfassungsgericht monierte sodann im Urteil zum BKA-Gesetz am 20. April 2016, dass die dem BKA eingeräumten Überwachungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus keine ausreichenden Vorkehrungen zum Schutz des Kernbereichs enthielten[801] und verpflichtete den Gesetzgeber dazu, immer dann wirksame Schutzregelungen zu schaffen, wenn die Überwa-

795 BVerfGE 6, 32 ff.
796 BVerfGE 6, 32 ff.; *Denninger*, ZRP 2004, 101.
797 BVerfGE 6, 32, 41; st. Rspr. Vgl. BVerfGE 109, 279, 313; BVerfGE 141, 220, 276; BVerfG, NJW 2020, 2235, Rn. 200.
798 *Gercke*, GA 2015, 339, 342.
799 BVerfGE 34, 238, 245 f.
800 BVerfGE 80, 367, 374.
801 BVerfGE 141, 220, Rn. 145 ff.

chungsmaßnahmen typischerweise kernbereichsspezifische Informationen erfassen könnten.[802] Gewährleistet werden müsse der Kernbereichsschutz durchgehend sowohl auf der Erhebungsebene als auch der Auswertungs- und Verwertungsebene.[803] Die genauen Regelungen können für verschiedene Überwachungsmaßnahmen sodann aber je nach Art der Maßnahme sowie ihrer Eignung, kernbereichsspezifische Daten zu erfassen differierend ausgestaltet werden.[804]

b) Verfassungsrechtliche Grundlage

Verfassungsrechtlich entstammt der unantastbare Kernbereich der privaten Lebensgestaltung der Wesensgehaltsgarantie der Grundrechte aus Art. 19 Abs. 2 GG, dem aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleiteten allgemeinen Persönlichkeitsrecht und der Menschenwürdegarantie des Art. 1 GG.[805] Ausgangspunkt der inhaltlichen Ausgestaltung des unantastbaren Kernbereichs stellt sodann primär der Menschenwürdegehalt des Freiheitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar.[806] Das allgemeine Persönlichkeitsrecht soll neben den spezielleren Freiheitsrechten den Schutz und die Erhaltung der allgemeinen Persönlichkeitsentfaltung sowie der „engeren persönlichen Lebensgestaltung" gewährleisten.[807] Dabei wird zwischen dem hieraus entspringenden absolut geschützten Kernbereich privater Lebensgestaltung und dem um ihn herum liegenden Bereich privater Lebensgestaltung unterschieden. Zweiterer kann bei einem überwiegenden Interesse der Öffentlichkeit unter strikter Wahrung des Verhältnismäßigkeitsgebots eingeschränkt werden.[808] Bei einer Kernbereichsbetroffenheit wiederum haben selbst überragend wichtige Interessen der Allgemeinheit zurückzustehen und können einen Eingriff in die-

802 BVerfGE 141, 220, Rn. 123.
803 BVerfGE 120, 274, 337; BVerfGE 129, 208, 247; BVerfGE 141, 220, Rn. 200; BVerfG, NJW 2020, 2235, Rn. 205.
804 BVerfGE 120, 274, 337; BVerfGE 129, 208, 245.
805 BGHSt 31, 296, 299 f. mit Verweis auf BVerfGE 27, 1, 6; BVerfGE 34, 238, 245; *Dammann*, Der Kernbereich der privaten Lebensgestaltung, S. 143 f.; *Kutscha*, NJW 2005, 20, 21.
806 *Eisenberg*, Beweisrecht der StPO, Rn. 387; *Lindemann*, JR 2006, 191, 192.
807 *Barrot*, Der Kernbereich, S. 25.
808 BVerfGE 27, 344, 351; BVerfGE 32, 373, 379; BVerfGE 33, 367, 376 f.; BVerfGE 65, 1, 43 f.

sen absolut geschützten Bereich nicht legitimieren.[809] Dabei können speziellere Grundrechte wie Art. 13 GG, Art. 4 GG oder Art. 6 GG den Kernbereichsschutz weiter konkretisieren und dessen Schutzbedürfnisses weiter erhöhen.[810] Seit jeher enthält das Grundgesetz im Rahmen des Geheimnisschutzes aus Art. 10 Abs. 1 GG, der Unverletzlichkeit der Wohnung in Art. 13 GG oder dem Schutz der Ehe und Familie in Art. 6 Abs. 1 GG, Schutzvorschriften zur Wahrung der Persönlichkeitsentfaltung.

c) Negative Kernbereichsprognose

Das Bundesverfassungsgericht zieht zur Bestimmung des Kernbereichs sowohl formale als auch inhaltliche Kriterien heran. Grundlegende Voraussetzung für die Einschlägigkeit des Kernbereich sind ein höchstpersönlicher Akt, mithin die Frage in welcher Art und Intensität ein Sachverhalt die Sphäre anderer oder die Belange der Gemeinschaft berührt sowie ein subjektiver Geheimhaltungswille.[811]

Hinsichtlich der inhaltlichen Ausgestaltung des Kernbereichsschutzes ist zwischen den Indikatoren im Sinne der der negativen Kernbereichsprognose auf der Erhebungsebene nach § 100d Abs. 4 S. 1 StPO und den tatsächlichen Definitionsmerkmalen des Kernbereichs zu differenzieren. Lediglich die Definitionsmerkmale (Höchstpersönlichkeit und Geheimhaltungswille) wiederum würden auf der Verwertungsebene bestimmen, ob eine Äußerung tatsächlich dem Kernbereich zuzuordnen ist.[812] Die durchzuführende Kernbereichsprognose fußt dagegen im Schwerpunkt auf der zu erwartenden Thematik der Kommunikation, dem Vertrauensverhältnis der miteinander Kommunizierenden, der Anzahl der Kommunizierenden und der räumlichen Situation.[813]

809 BVerfGE 109, 279, 313; BVerfGE 141, 220, Rn. 120.
810 BVerfGE 109, 279, 326; vgl. auch *Weißer*, GA 2006, 148, 161.
811 BVerfGE 80, 367, 374; BVerfG, Beschluss vom 26. Juni 2008 – 2 BvR 219/08 -, Rn. 18 = BVerfGK 14, 20, 24; BVerfG, Beschluss vom 18. April 2018 – 2 BvR 883/17 -, Rn. 27; *Beulke/Swoboda*, Strafprozessrecht, Rn. 415; *Amelung*, NJW 1990, 1753, 1755.
812 *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 77.
813 BVerfGE 109, 279, 320; BVerfG, NJW 2007, 2753, 2754 f.

aa) Indikatoren der negativen Kernbereichsprognose

Im Rahmen der Entscheidungen zur Wohnraumüberwachung mittels eines großen Lauschangriffs[814] entwickelten das Gericht erstmals Indikatoren zur Frage, wie wahrscheinlich eine Kernbereichsbetroffenheit während der Datenerhebung ist.

(1) Räumliche Situation

Die räumliche Situation des Überwachten betrachtend, leuchtet es ein, dass für Gespräche an Orten, die typischerweise oder im Einzelfall als Rückzugsbereich der privaten Lebensgestaltung dienen, eine starke Vermutung für die Zuordnung zum Kernbereich besteht.[815] Dabei ist eine Unterscheidung nach einzelnen Räumen innerhalb einer Privatwohnung nicht angezeigt, da der Betroffene jeden Raum seiner Wohnung als gleich überschaubar betrachten wird und sich vor allen Dingen auch überall gleich unbeobachtet fühlt.[816] Dagegen soll zu Arbeits- und Geschäftsräumen abzugrenzen sein. Die in solchen Räumen ablaufende Kommunikation deute auf einen Sozialbezug hin.[817] Allerdings sei zu beachten, dass das Charakteristikum als Arbeits- oder Geschäftsraum alleine nicht ausreiche, um einen Sozialbezug zu begründen.[818] Sind die Geschäftsräume für den Publikumsverkehr beispielsweise geschlossen oder handelt es sich um einen abgetrennten Arbeitsraum im eigenen Wohnhaus, so könne auch die an diesen Orten ablaufende Kommunikation schützenswert sein.[819] Aus der neusten Entscheidung des Bundesverfassungsgericht zur Verfassungsmäßigkeit des BKAG lässt sich darüber hinaus eine Ausweitung der räumlichen Komponente des Kernbereichs feststellen.[820] Hinsichtlich § 20g BKAG, der diverse Überwachungsmöglichkeiten außerhalb der Wohnung beinhaltet, verneinte der erste Senat die Verfassungsmäßigkeit der Vorschrift, da diese keine Regelungen zum Kernbereichsschutz enthielt.[821] Daraus ist zu folgern, dass der Senat nunmehr davon ausgeht,

814 BVerfGE 109, 279.
815 BVerfGE 109, 279, 321; *Baldus*, JZ 2008, 218, 220.
816 BVerfGE 109, 279, 321.
817 *Bludovsky*, Rechtliche Probleme beim Lauschangriff, S. 79.
818 BT-Drs. 18/12785, S. 57.
819 Vgl. zu Art. 13 GG, § 5, B., II), 1) a).
820 *Dürr*, JA 2019, 432, 435.
821 BVerfGE 141, 220, Rn. 175.

dass es auch außerhalb der Wohnung typischerweise zu kernbereichsrelevanten Gesprächen kommen kann. Es stehe danach außer Frage, dass höchstvertrauliche Situationen, die dem Kernbereich privater Lebensgestaltung zuzuordnen sein könnten auch im Auto, abseits in einem Restaurant, oder bei einem zurückgezogenen Spaziergang erfasst werden können.[822] Gleichwohl wurde diese Erweiterung in den Sondervoten der Richter *Eichberger* und *Schluckebier* kritisiert. Während *Eichberger* es jedenfalls für nicht typischerweise gegeben erachtet, dass es bei Überwachungsmaßnahmen im öffentlichen Raum zur Erfassung kernbereichsspezifischer Situationen kommt, hält *Schluckebier* Gespräche außerhalb von Wohnungen für grundsätzlich nicht schutzwürdig.[823] Gerade angesichts dessen, dass eine Vielzahl an Themen vorstellbar sind, die sich möglicherweise gerade nicht in der Wohnung besprechen lassen, weil dort die Privatsphäre gegenüber anderen Familienmitgliedern nicht gewahrt sein könnte, ist diese Erweiterung allerdings notwendig.[824] Insbesondere wäre ansonsten auch eine Benachteiligung derer zu befürchten, die mit ihren Familien in räumlich beengten Verhältnissen leben oder weitergehend über keine Wohnung verfügen. Ein auf die Wohnung beschränkter Schutz, würde diese Menschen grundlos vom Kernbereichsschutz ausschließen.[825]

(2) Vertrauensverhältnis der Kommunizierenden

Daneben spricht auch eine Kommunikation zwischen Personen des höchstpersönlichen Vertrauens für eine Zuordnung zum Kernbereichsschutz. Bei Gesprächen zwischen solchen Personen besteht eine widerlegbare Vermutung, dass die in einem solchen Gespräch entstammenden Informationen dem Kernbereich höchstpersönlicher Lebensführung angehören.[826] Insbesondere Art. 6 GG bringt zum Ausdruck, dass sowohl die Ehe als auch die Familie im Allgemeinen für die Kommunikation im höchstpersönlichen Bereich eine besondere Bedeutung haben. Die Mög-

822 BVerfGE 141, 220, Rn. 176.
823 BVerfGE 141, 220, 359 (abw. Meinung *Eichberger*); BVerfGE 141, 220, 367 f. (abw. Meinung *Schluckebier*); *Starck*, NdsVbl 2008, 145, 148.
824 Bereits vor dem Urteil des BVerfG mit eindeutigem Votum *Poscher*, JZ 2009, S. 269, 271; *Weißer*, GA 2006, 148, 161; *Kretschmer*, HRRS 2010, 551, 557; *Schwabenbauer*, Heimliche Grundrechtseingriffe, S. 260, *Zimmermann*, GA 2013, 162, 169.
825 *Poscher*, JZ 2009, S. 269, 271.
826 BVerfGE 141, 220, Rn. 128.

lichkeit der thematisch unbegrenzten, da vertrauenswürdigen Kommunikation, mit dem Ehepartner gründet nicht zuletzt auf der Annahme, dass der Vorgang nicht von Dritten erfasst werden kann.[827] Hinsichtlich des zwischen den Kommunizierenden möglicherweise bestehenden Vertrauensverhältnisses stellt sich die Frage, anhand welcher Maßstäbe ein solches zu klassifizieren ist. Eine mögliche Orientierung soll die Aufzählung in den §§ 52, 53 StPO bieten.[828] Damit wäre bei sämtlichen zeugnisverweigerungsberechtigten Personen, seien es auch nur entfernte Verwandte oder in § 53 StPO genannte Berufsgeheimnisträger, von einer erhöhten Kernbereichswahrscheinlichkeit auszugehen.[829] Dem wird entgegengehalten, dass Sinn und Zweck der §§ 52 ff. StPO nicht der Schutz des Vertrauensverhältnisses zwischen den dort genannten Angehörigen und Beschuldigten sei, sondern vielmehr der Zwangslage der Zeugen, die einer Wahrheitspflicht unterliegen und befürchten müssen einen Angehörigen zu belasten.[830] Dem wird entgegnet, dass § 52 StPO mittelbar sehr wohl auch das Vertrauensverhältnis zwischen den Gesprächspartner schütze.[831] Der Betroffene dürfe sich in der Kommunikation darauf verlassen, dass sein Gesprächspartner die ihm zugetragenen Informationen nicht preisgeben müsse, wodurch er sich womöglich eher zu einem vertraulichen Gespräch bereit fühle.[832] Somit komme § 52 StPO durchaus eine unmittelbare Auswirkung auf das innerhalb zwischenmenschlicher Beziehungen bestehende Vertrauensverhältnis zu, indem die Norm die freie und unbesorgte Kommunikation garantieren wolle.[833] Diesem Verständnis folgend wäre der im Rahmen des § 52 StPO vielzitierte „Schutz der Familienbande“[834] nicht lediglich dahingehend zu verstehen, den Zeugen innerhalb einer Familie vor Konfliktsituationen zu schützen, sondern ein umfassendes Biotop zu schaffen, in welchem familiäre Vertrauensbeziehung auch aktiv durch vertrauliche Gespräche gelebt werden können.

Dies missachtet aber, dass es schlicht nicht abschließend und vor allen Dingen abstrakt nicht möglich ist, zu kodifizieren, zwischen welchen

827 BVerfGE 109, 279, 322.
828 so *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, S. 99 ff., anders *ders*., KJ 2005, 276, 280.
829 *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, S. 99 ff.
830 BVerfGE 109, 279, 322.
831 *Son*, Heimliche Polizeieingriffe, S. 200 f.
832 *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, S. 101; *Son*, Heimliche Polizeieingriffe, S. 200 f.
833 *Weißer*, GA 2006, 148, 154.
834 BGHSt 11, 213, 216; BGHSt 38, 96, 99.

Personen ein besonderes Vertrauensverhältnis besteht. Dass ein solches schließlich auch zwischen nicht in § 52 StPO normierten Personen bestehen kann, ist ureigenste Konsequenz des individuellen Persönlichkeitsrechts, welches es durch die Normierung des Kernbereichs gerade zu schützen gilt. Insofern könnte § 52 StPO lediglich eine widerlegbare Vermutung zugunsten der Betroffenheit des Kernbereichs aufstellen. Dabei gilt es zu beachten, dass es gleichfalls denkbar ist, dass mit anderen Personen als den in § 52 StPO genannten, beispielsweise einem engen Freund, ein vertrauensvolles Gespräch geführt wird.[835] Nicht selten werden solche nicht in den §§ 52 ff. StPO aufgeführten Personen – wie beispielsweise ein jahrelanger Freund – womöglich gar erster Ansprechpartner für eine höchstpersönliche Angelegenheit darstellen. Ob ein solches besonderes Vertrauensverhältnis vorliegt, muss daher stets am konkreten Einzelfall entschieden werden.[836] Es obliegt nicht dem Staat, den Einzelnen für eine vertrauensvolle Kommunikation an die eigene Familie zu verweisen, sondern ein jeder muss das Recht haben, sich frei an die Personen wenden zu können, denen der Betroffene tatsächlich uneingeschränkt vertraut.[837] Ebenso sind Gespräche innerhalb einer zerrütteten Familie oder schlicht in Familien vorstellbar, die zueinander ein distanziertes Verhältnis pflegen. Bei sämtlichen Familienangehörigen, noch dazu bei entfernten Verwandten, von einem solch engen Vertrauensverhältnis auszugehen, würde in dieser Pauschalität das in der Realität zu erwartende Familienbild übersteigen.[838] Unabhängig dieser faktischen Umstände, überzeugt es in der Tat auch nicht, dass einfache Gesetzesrecht zur inhaltlichen Ausgestaltung des Verfassungsrechts heranzuziehen. Gleich ob dies mit der Normenhierarchie[839] oder der ansonsten bestehenden Möglichkeit mittels einer Änderung des einfachen Rechts eine Beeinflussung des Verfassungsrechts zu erzielen[840], begründet wird, müssen verfassungsrechtliche Grundsätze wie

835 BVerfGE 109, 279, 322; *Bludovsky*, Rechtliche Probleme beim Lauschangriff, S. 87; *Gusy*, JuS 2004, 457, 460.

836 *Gercke*, GA 2015, 339, 343; a.A.: *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, S. 104, der unter Berücksichtigung ansonsten entstehender Abgrenzungsschwierigkeiten für eine abschließende Heranziehung der §§ 52, 53 StPO plädiert.

837 *Fink*, Intimsphäre und Zeugenpflicht S. 174.

838 *Hauck*, Heimliche Strafverfolgung, S. 473; *Fink,* Intimsphäre und Zeugenpflicht S. 174.

839 *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 144.

840 *Bludovsky,* Rechtliche Probleme beim Lauschangriff, S. 85.

der höchstpersönlichen Kernbereich ihren Inhalt aus der Verfassung selbst beziehen. Im Gesamten kann der Kernbereichsschutz in personeller Hinsicht weiter gehen als es durch § 52 ff. StPO den Anschein hätte, gleichfalls aber auch enger sein, als es bei einer schablonenartigen Übertragung des § 52 StPO der Fall wäre. Einen tatsächlichen Anhaltspunkt kann § 52 StPO für diese Einordung nicht liefern.

(3) Anzahl der Kommunizierenden

Teilweise wird angenommen, dass auch die Anzahl der an der Kommunikation beteiligten ein Parameter für die Beurteilung der Kernbereichsrelevanz sei.[841] Angesichts dessen, dass die Interaktion mit anderen Menschen gerade Ausfluss des Bedürfnisses eines einzelnen Menschen ist, in sozialen Bezügen existieren zu wollen,[842] kann sich die Höchstpersönlichkeit einer Äußerung nicht bereits dadurch verringern, dass diese in Gegenwart dritter Personen getätigt wird. Durch das Hinzukommen weiterer Menschen wird daher der Schutzkreis der Höchstpersönlichkeit nicht automatisch peu à peu verlassen.[843] Gleichwohl steigt mit der Anzahl der Kommunikationspartner jedenfalls abstrakt das Risiko, dass Teile der Kommunikation nach außen dringen. Sind mehrere Personen an einer Kommunikation beteiligt, liegt es in der Natur der Sache, dass der Betroffene nicht zu allen die gleich enge Vertrauensbeziehung innehat. Gelangt eine vertrauliche Information schließlich nach Außen, ist für den Betroffenen beispielsweise bereits nicht mehr nachzuvollziehen, über welchen Weg dies geschah. Gleichsam reduzieren mehrere Gesprächspartner das Risiko für den Einzelnen als „Maulwurf" enttarnt zu werden. Die Gesprächssituation, in welcher der Kommunizierende trotz der Interaktion mit einem Dritten die vermeintlich sicherste Position innehat, wird daher in der Regel das klassische „vier Augen" Gespräch bleiben. Davon ausgehend, dass dies dem Betroffenen bewusst sein muss, erscheint es gemessen an der allgemeinen Lebenserfahrung korrekt, eine höhere Anzahl an Gesprächsteilnehmern als Indiz für eine nicht vorhandene Kernbereichsrelevanz anzusehen. Eine größere, zuweilen nicht sofort überschaubare, Personenanzahl steigert die

841 *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, S. 92; *Gercke*, GA 2015, 339, 344.
842 BVerfGE 80, 367, 374; BVerfGE 109, 279, 319; BVerfGE *125, 175, 223*; BVerfGE 132, 134, Rn. 64.
843 *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, S. 92.

Gefahr, dass höchstpersönliche Vorgänge trotz eines möglicherweise entgegenstehenden Willens nach außen dringen.[844]

(4) Thematik

Hinsichtlich des Inhalts eines Gesprächs ist für eine Zuordnung zum Kernbereich entscheidend, inwiefern innerste Gefühle oder Thematiken, die üblicherweise aus Sicht eines objektiven Betrachters exklusiv im Kreis engster Vertrauter besprochen werden, Gegenstand der Kommunikation sind. Die genaue Zuordnung erfolgt jedoch undurchsichtig und wenig trennscharf.[845] Dies verdeutlicht die erste Tagebuchentscheidung des BVerfG vom 14. September 1989, in welcher vier der acht Richter des zweiten Senats die Inhalte rund um das dem Fall zugrunde liegende Tagebuch dem höchstpersönlichen Kernbereich zuordneten und damit von einer Unverwertbarkeit ausgingen, während die restlichen vier Richter den Inhalt der Aufzeichnungen für verwertbar erachteten.[846] Es wird deutlich, dass entscheidend letztlich eine bloße Gewichtung ist, ob dem Strafverfolgungsanspruch des Staates oder dem Persönlichkeitsrecht des Einzelnen der Vorrang zu geben ist. So wird ausgeführt, dass eine Verletzung der Menschenwürde nicht in Betracht komme, wenn die Auswertung Aufschluss über Ursachen und Hintergründe der Straftat geben könne und dazu der Verfasser seine Gedanken aus seinem Inneren entlasse und schriftlich manifestiert habe.[847] Die die Verwertung ablehnenden Verfassungsrichter stellen dagegen in den Vordergrund, dass die Aufzeichnungen aufgrund ihrer Art und Weise der geheimen Aufbewahrung und ihres höchstpersönlichen Charakters von der Verwertung ausgenommen bleiben müssen.[848] Aufgrund dieser Stimmgleichheit konnte nicht festgestellt werden, ob die Verwertung der Aufzeichnungen des Beschwerdeführers in dem gegen diesen laufenden Strafverfahren gegen das Grundgesetz verstößt, sodass die durch die Strafgerichte vorgenommene Beweiswürdigung nicht beanstandet wurde.[849] Zu einer erhöhten Rechtsunsicherheit führt dabei, dass das Urteil deutlich vor Augen führt, dass die entschei-

844 *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, S. 93.
845 *Eisenberg*, Beweisrecht der StPO, Rn. 389; *Lucke,* HRRS 527, 531.
846 BVerfGE 80, 367.
847 BVerfGE 80, 367, 376 f.
848 BVerfGE 80, 367, 381.
849 BVerfGE 80, 367, 376.

dende Abwägung hinsichtlich einer Zuordnung zum höchstpersönlichen Kernbereich mehr von persönlichem Dafürhalten als von handfesten juristischen Grundsätzen geprägt ist.[850] Es ist der Einordung eines persönlichen Vorgangs in verschiedene Sphären zwar immanent, dass verschiedene Vorgänge von verschiedenen Personen unterschiedlich stark gewichtet werden und folglich auch in unterschiedliche Sphären eingeordnet werden (sog. Relativität der Sphären).[851] Einen solch subjektiven Einschlag in einer grundlegenden Frage der Beweisverwertbarkeit und damit im Zweifelsfall in einer entscheidenden der Verurteilung vorgelagerten Frage ist mit dem Rechtsstaatlichkeitsprinzip nur schwerlich zu vereinbaren.

bb) Verhältnis der Indikatoren

Offen bleibt bisweilen das Verhältnis dieser Indikatoren zueinander. Dabei ist gerade die Gewichtung der einzelnen Parameter zentraler Bestandteil zur Einordung des zu überwachenden Verhaltens und damit zur Definition der Kernbereichsprognose i.S.d. § 100d Abs. 1 StPO. Trennscharfe Abgrenzungskriterien, inwiefern ein Verhalten im Lichte dieser Indikatoren als ein solches des höchstpersönlichen Kernbereichs einzuordnen wäre, bestehen nicht. In der Literatur heißt es zuteilen, dass während die Kriterien der räumlichen Situation, des Vertrauensverhältnisses und der Anzahl der Kommunizierenden eine bloße Indizwirkung zur Kernbereichszugehörigkeit geben können, vor allen Dingen die Thematik des Gesprächs das entscheidende Merkmal darstelle.[852] Problematisch daran ist allerdings, dass die Thematik der ablaufenden Kommunikation gleichfalls den am schwersten vorherzusehenden Indikator darstellen wird. Zum Zeitpunkt der Anordnung der Überwachungsmaßnahme und damit zum Zeitpunkt, zu dem die negative Kernbereichsprognose getroffen werden muss, wird eher feststehen in welchem Vertrauensverhältnis sich die in der überwachten Räumlichkeit aufhaltenden Personen befinden. Sofern die polizeilichen Ermittlungen daher keine Anhaltspunkte zur erwartbaren Gesprächsinhalten hervorbrachten, müssen vor allem die bekannten Indikatoren des Vertrauensverhältnisses und des räumlichen Ortes im Rahmen

850 *Amelung*, NJW 1990, 1753, 1755; ähnlich auch *Martini*, JA 2009, 839, 844; *Kleb-Braun*, CR 1990, 344, 346.
851 *Desoi/Knierim*, DÖV 2011, 398, 400; *Hufen*, Jus 2010, 1, 9; *Albers*, informationelle Selbstbestimmung, S. 211.
852 FS-Fischer/*Kudlich*, 723, 729.

der negativen Kernbereichsprognose gewichtet werden. Eine Maßnahme wird eher zu unterbleiben haben, wenn sich der Beschuldigte, gemeinsam mit einer Person, zu der er aufgrund konkreter Anhaltspunkte eine höchst vertrauensvolle Beziehung pflegt, an einem geschützten Ort wie der Privatwohnung aufhält. Den gegenteiligen Fall wird die Situation darstellen, in welcher sich der Tatverdächtige in einem Geschäftsraum mit einer ihm nicht nahestehenden Person treffen wird. Neben diesen Fallkonstellationen werden die Ermittlungsbehörden jedoch auch mit Fällen konfrontiert werden, in welchen in einer Privatwohnung ein Treffen zwischen zwei Geschäftspartnern stattfindet, die zueinander in keiner Vertrauensbeziehung stehen. Während die räumliche Komponente für eine Kernbereichsbetroffenheit spricht, ist von einer solchen bei Betrachtung personellen Umstände nicht auszugehen.

Daher stellt sich nun die Frage, welcher der Komponenten das höhere Gewicht beizumessen ist. Das Bundesverfassungsgericht spricht hinsichtlich des räumlichen Parameters von einer Funktion als Rückzugsbereich der privaten Lebensgestaltung, die der Privatwohnung aufgrund ihrer Vertrautheit und Geborgenheit zukomme.[853] Daran anknüpfend wird angenommen, dass diese Vertrautheit und Geborgenheit aufgehoben sei, wenn der Betroffene seinen privaten Rückzugsbereich für fremde Personen öffnet.[854] Dies wird damit begründet, dass, sofern sich ein Arbeitskollege oder flüchtiger Bekannter in der Wohnung aufhält, nicht mit höchstpersönlichen Handlungen zu rechnen sei. Zu solchen hierzu zu zählenden Handlungen oder Äußerungen würde es gerade nicht kommen, wenn auch Personen anwesend sind, die nicht zum Kreis des engsten Vertrauens zählen.[855] Zwar ist dem durch Art. 13 GG gebotenen Schutz eine Einstufung anhand der sich in der Wohnung befindlichen Personen fremd, dennoch erscheint es im Lichte der negativen Kernbereichsprognose zielführend, mittels des von Fall zu Fall individuell ausgestalteten Indikators der Vertrauensbeziehung die lediglich typisierende Indizwirkung der räumlichen Komponente einzuschränken. Durch eine höhere Gewichtung der individuellen Komponenten kann dem Kernbereichsschutz daher im jeweiligen Einzelfall besser entsprochen werden. In die gleiche Richtung tendiert auch das Bundesverfassungsgericht, das anmerkt, dass die Wahrscheinlich-

853 BVerfGE 109, 279, 321.

854 *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 150 f.

855 *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 150 f.

keit durch Überwachungsmaßnahmen in den Kernbereich einzudringen, davon abhängt, welche Personen sich in der überwachten Wohnung aufhalten.[856] Sofern der zu erwartende Gesprächsinhalt zum Zeitpunkt des Aufstellens einer Kernbereichsprognose nicht bekannt ist, ist primär das Verhältnis der sich in einer Wohnung aufhaltenden Personen entscheidend, während dem Umstand, dass sich diese Personen dabei in einer Privatwohnung aufhalten nur sekundäre indizielle Wirkung zukommt.[857]

d) Einschränkungen des Kernbereichs

Selbst bei einer Kommunikation, die grundsätzlich für eine Zuordnung zum Kernbereich in Frage kommt, wird dessen tatsächliche Reichweite zu Gunsten einer effektiven Strafverfolgung eingeschränkt.[858] Erstmals wurde dies deutlich als das BVerfG in der Tagebuchentscheidung dem Kernbereich nicht gemeinhin sämtliche persönlich preisgegeben Informationen zuordnete.[859] Denn die Verfassung erfordert es nicht, Tagebücher und andere private Aufzeichnungen schlechthin der Verwertung zu entziehen. Maßgeblich ist für diese Entscheidung der Charakter und die Bedeutung des entsprechenden Inhalts.[860] Je deutlicher eine getätigte Äußerung folglich Sozialbezug aufweist, desto weniger erscheint es möglich diese Äußerung noch dem Kernbereich zuzuordnen.[861] Die Intensität des Sozialbezugs kann dabei durch unterschiedliche, im Folgenden zu betrachtende, Punkte zum Ausdruck kommen.

aa) Art des Gesprächs

Insofern wird bereits differenziert, ob der Betroffene ein Zwie- oder Selbstgespräch führt. Das Zwiegespräch unterscheidet sich vom Selbstgespräch dadurch, dass nur die Äußerungen im Rahmen eines Selbstgespräches dazu bestimmt sind, von anderen nicht zur Kenntnis genommen zu werden.[862] Dieser Unterschied führt dazu, dass die in einem Zwiegespräch

856 BVerfGE 109, 279, 321.
857 *Wolter* in: SK-StPO, § 100c StPO, Rn. 61.
858 Vgl. BVerfGE 80, 367, 374 f.
859 BVerfGE 80, 367, 374 f.
860 BVerfGE 80, 367, 374 f.
861 BVerfGE 80, 367, 374; BVerfGE 109, 279, 314.
862 BGH, NJW 2005, 3295, 3297.

getroffenen Äußerungen weniger schützenswert seien.[863] Dass das Selbstgespräch prägende Kriterium der Unbewusstheit einer Äußerung wird im Rahmen eines Zwiegesprächs – sei es auch in der eigenen Wohnung – nicht mehr gegeben sein, da der sich Äußernde überlegen wird, ob er eine Information aus seinem „forum internum" einer dritten Person zugänglich machen will. Dabei kann allerdings auch eine bewusst vorgenommene Äußerung sehr wohl dem Kernbereich zuzuordnen sein. Es wäre mit der Menschenwürde nicht vereinbar, wenn der Einzelne sich keiner weiteren Person derart vertrauen könnte wie sich selbst. Auch an dieser Stelle ist abermals darauf zu verweisen, dass sich der Mensch gerade in seinen sozialen Bezügen verwirklicht.[864] Diese Aussage des Bundesverfassungsgerichts ernstnehmend, muss es sodann möglich sein, mit einem auserwählten Dritten ebenso offen wie mit sich selbst sprechen zu können.[865]

Umso bedeutender als die Art des Gespräches ist daher die Frage nach dem Gesprächspartner und die zwischen den Beteiligten bestehenden Vertrauensverhältnisses. Gerade der Ehepartner hat für die Kommunikation im höchstpersönlichen Bereich eine herausragende Bedeutung. Gleiches gilt für Gespräche mit anderen engsten Familienangehörigen, etwa Geschwistern und Verwandten in gerader Linie oder anderen Personen, zu denen eine vergleichbare Vertrauensbeziehung besteht.[866] In solchen Situation wird es vielfach der Fall sein, dass der Betroffene seinem Gegenüber sprichwörtlich „die Seele ausschüttet". Ferner ist es vorstellbar, dass in einem hochemotionalen Gespräch das Kriterium der Unbewusstheit einer Äußerung wieder in den Vordergrund rückt. Es leuchtet nicht ein, weshalb ein Einblick in das Seelenleben einer Person in einem Selbstgespräch, jedoch nicht auch in einem Zwiegespräch erfolgen kann.[867] Die Möglichkeit, Einblicke in das Innere einer Person zu erhalten, ist in einem Zwiegespräch möglicherweise sogar bedeutend höher, gerade dann, wenn der Kommunizierende möglicherweise das Gefühl hat, sich durch das Offenbaren seiner Gefühlswelt von Ballast zu befreien. Allein die Art eines Gesprächs als Zwiegespräch führt daher nicht zur Begründung eines der-

863 *Ernst/Sturm*, HRRS 2012, 374, 380.
864 BVerfGE 80, 367, 374; BVerfGE 109, 279, 319; BVerfGE *125, 175, 223*; BVerfGE 132, 134, Rn. 64.
865 Vgl. GS-Lisken/*Bergemann*, 69, 74.
866 BVerfGE 109, 279, 322; BVerfGE 141, 220, Rn. 121.
867 Zutreffend *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 89; a.A.: *Traub*, Verwertbarkeit von Selbstgesprächen, S. 122.

artigen Sozialbezug, der die Kommunikation als weniger schützenswert erscheinen ließe.

bb) Inhalt: Straftatvorbehalt

Regelmäßig ist es der Bezug einer Äußerung zu Straftaten, weshalb ein Gespräch mit potentieller Kernbereichsrelevanz letztlich nicht als absolut schutzwürdig eingestuft wird. Sofern die Strafverfolgungsbehörden aufgrund Vorfeldermittlungen davon ausgehen dürfen, dass ihre Überwachungsmaßnahmen Angaben zu Straftaten enthalten könnten, soll der Kernbereichsschutz zurücktreten, da durch dessen grundrechtliche Ausprägung schließlich *„die Entfaltung, nicht der Verfall der Persönlichkeit [geschützt werden soll]"*[868]. Mit dem sog. Straftatvorbehalt berücksichtigen die Gerichte das Allgemeininteresse an einer wirksamen Strafverfolgung bereits bei der Definition des Kernbereichs. Im Einzelfall muss daher auch der Kernbereichsschutz diesen entgegenstehenden Gemeinwohlinteressen weichen. Vor allem Tagebuchaufzeichnungen, Zwiegespräche, aber auch Selbstgespräche waren unter diesem Gesichtspunkt regelmäßig Gegenstand vergangener Entscheidungen.

(1) Im Rahmen der Tagebuchaufzeichnung

(1.1) Tagebuchentscheidungen des BGH 1964 und 1988

Schon im zurückliegenden Jahrhundert beschäftigte die Gerichte der beweisrechtliche Umgang mit Tagebuchaufzeichnungen. In der ersten Tagebuchentscheidung des BGH aus dem Jahre 1964 konnte der Verfasser aufgrund seiner Tagebuchaufzeichnungen der Lüge vor Gericht überführt werden, was aufgrund der Vereidigung des Betroffenen in strafrechtlicher Hinsicht einen Meineid darstellte.[869] Bereits damals wurde hinsichtlich einer schriftlichen Aufzeichnung festgestellt, dass mit einer solchen – im Unterschied zu Gesprächen – gerade kein Kundgebungszweck gegenüber den Gesprächspartnern einhergeht. Vielmehr seien Aufzeichnungen intimer Art regelmäßig von vornherein nicht zur Kenntnis anderer bestimmt. Es müsse jedermann freistehen ohne die Befürchtung, dass solche Auf-

868 Bereits BGH, NJW 1964, 1139, 1143.
869 BGH, NJW 1964, 1139 ff.

zeichnungen unbefugterweise verwertet werden, Empfindungen, Gefühle, Ansichten und Erlebnisse beliebig für sich festzuhalten.[870] Dementsprechend ordneten die Richter die aus der Aufzeichnungen entspringenden Informationen zwar einem „Geheimbereich" zu; dieser war jedoch noch nicht gleichbedeutend mit dem heutigen Kernbereich. So nahmen die Richter gleichwohl der Zuordnung zum „Geheimbereich" eine Abwägung mit den widerstreitenden Interessen der Strafverfolgung im Einzelfall vor.[871] In der zweiten Tagebuchentscheidung des BGH im Jahr 1988 wurde zwar festgestellt, dass die Notizen des sich mit seinen Frauenproblemen auseinandersetzenden Beschuldigten höchstpersönlichen Inhalt haben, dies jedoch in Fällen schwerster Kriminalität gleichwohl keinen Kernbereichsschutz begründen könne.[872]

(1.2) Erste Tagebuchentscheidung des BVerfG vom 14.09.1989 – 2 BvR 1062/87

Mit der durch den BGH daher bestätigten Verurteilung aufgrund eines Heimtückemordes musste sich sodann der zweite Senat des BVerfG im Rahmen seiner ersten Tagebuchentscheidung befassen. Der Senat bestätigte die BGH-Rechtsprechung dahingehend, dass eine Zuordnung zum Kernbereich aufgrund der schriftlichen Fixierung der Gedanken, jedenfalls aber, da die Aufzeichnungen über die Rechtssphäre des Verfassers hinaus die Sphäre Dritter tangiere, nicht in Betracht komme.[873] Da sich die Schilderungen des Betroffenen allerdings lediglich mit der zur Straftat führenden Vorgeschichte mitsamt den hierfür ursächlichen Hintergründen befasste, gab es zwischen den acht Richtern keinen Konsens, ob der geforderte „unmittelbare Straftatbezug" im hiesigen Fall auch tatsächlich vorlag. Unter Bezug darauf, dass auch die Ursachen und Hintergründe zur Straftat „die Wurzeln der Tat" darlegen und somit Erkenntnisse über die Persönlichkeit des Täters liefern würde, hielten die vier Richter der obsiegenden Auffassung dies für einen unmittelbaren Tatbezug ausreichend.[874] Vom Bundesverfassungsgericht wurde damit erstmalig bestätigt, dass letztlich auch in Fällen eines nur „mittelbaren Straftatenbezuges", trotz eines

870 BGH, NJW 1964, 1139, 1142.
871 BGH, NJW 1964, 1139, 1143 f.
872 BGH, NJW 1988, 1037, 1038.
873 BVerfGE 80, 367, 374.
874 BVerfGE 80, 367, 377.

an sich höchstpersönlichen Vorgangs, der Kernbereich nicht einschlägig ist und stattdessen im Wege einer Abwägung über die Verwertbarkeit der Informationen zu entscheiden sei.

Die die Entscheidung tragende Rechtauffassung überzeugt dabei nicht vollumfänglich. Richtig ist zweifelsfrei, dass der Betroffene durch das Niederschreiben der Informationen diese aus seinem innersten Gedankenkreis entließ und dies im Rahmen der Kernbereichseingrenzung zu berücksichtigen ist. Die Zugehörigkeit zum Kernbereich auf Grund dessen eingehender zu problematisieren, erscheint daher angemessen. Problematisch werden die Ausführungen der tragenden Auffassung allerdings, wenn im Sinne des rechtsstaatlichen Auftrags der Wahrheitserforschung sich die Ermittlungen auch „auf die Persönlichkeit des Tatverdächtigen, sein Vorleben und sein Verhalten nach der Tat" beziehen müsse, „um dem Schuldgrundsatz umfassend Rechnung tragen zu können".[875] Ohne dabei in Abrede zu stellen, dass selbstverständlich die Persönlichkeit und das Verhalten nach der Tat schuld- und strafzumessungsrelevante Umstände darstellen, so ist dennoch zu beachten, dass es gerade Ziel und Auftrag des Kernbereichs ist, gewisse Teile der Persönlichkeit nicht Teil eines Strafverfahrens werden zu lassen. Dies würde allerdings unterlaufen, wenn bereits die bloße Möglichkeit, Erkenntnisse über die Persönlichkeitsstruktur des Tatverdächtigen zu gewinnen ausreichend ist, um privaten Aufzeichnungen den Kernbereichsschutz zu versagen. Der Kernbereichsschutz wäre für das Strafverfahren dann praktisch nicht mehr von Relevanz, da eine Unterscheidung zwischen einem unantastbaren Kernbereich und einem Bereich der Abwägung wäre schlicht nicht mehr vorhanden wäre.[876] Denn schließlich gibt jede Erkenntnis über den psychischen Zustand, mithin über die Persönlichkeit eines Verdächtigen, neue Hinweise sowohl über die Schuldfähigkeit als auch darüber, ob er die Tat begangen haben könnte. Die Hürde zur Verwertbarkeit höchstpersönlicher Informationen wäre derart gering, dass der bloße Verdacht hinsichtlich einer Straftat geeignet wäre den Schutz des Kernbereichs zu beseitigen.[877]

875 BVerfGE 80, 367, 378.
876 BVerfGE 80, 367, 382 (abw. Meinung).
877 BVerfGE 80, 367, 382 (abw. Meinung).

(2) Im Rahmen eines Zwiegesprächs

(2.1) Urteil zum Großen Lauschangriff des BVerfG vom 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99

Nicht nur im Rahmen eines Tagebucheintrages, sondern auch bei der zwischen Menschen ablaufenden Kommunikation stellt sich regelmäßig die Frage, inwiefern die hier ablaufende Kommunikation dem Kernbereich zuzuordnen ist. Die Frage nach der Reichweite des Straftatvorbehalts steht auch hierbei häufig im Zentrum der Diskussion. Zu Recht folgte der erste Senat des BVerfG im Urteil zum Großen Lauschangriff diesbezüglich der nicht tragenden Auffassung aus der ersten Tagebuchentscheidung des BVerfG: Es soll gerade nicht jede Verknüpfung einer Äußerung und Verdacht einer begangenen Straftat zu einem derartigen Sozialbezug führen, dass der Äußerung der Schutz des Kernbereichs zu versagen wäre. Äußerungen, die ausschließlich innere Gefühle wiedergeben und keine Hinweise auf konkrete Straftaten enthalten, schließen den Kernbereichsschutz nicht bereits deshalb aus, da sie die Beweggründe für ein strafbares Verhalten offenbaren.[878] Wenngleich das Gericht für konkrete Hinweise auf Straftaten weiter einen Kernbereichsausschluss für angezeigt erachtete, so versteht es dieses Kriterium aber jedenfalls deutlich restriktiver. Angesichts dieses Urteils dürfte davon ausgegangen werden, dass die erste Tagebuchentscheidung des BVerfG aus dem Jahre 1989, gemessen an diesem Maßstab, mit der Bejahung des Kernbereichsschutzes geendet hätte. Schließlich befassten sich die damaligen Aufzeichnungen weder mit der konkreten Straftat noch mit Schilderungen der in Rede stehenden Straftat.[879]

(2.2) Zweite Tagebuchentscheidung des BVerfG vom 26.06.2008 – 2 BvR 219/08

Anstelle dieser Rechtsprechung im Rahmen der Zwiegespräche zu folgen, entschied wiederum der zweite Senat des BVerfG im Rahmen seiner zweiten Tagebuchentscheidung im Jahr 2008, dass auch Notizen des Betroffenen, die sich nicht auf die konkrete Straftat beziehen, sondern lediglich „konkrete Hinweise auf die Persönlichkeitsstruktur" enthielten, vom Kern-

878 BVerfGE 109, 279, 319.

879 BVerfGE 80, 367 ff.; *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 45.

bereichsschutz auszunehmen seien.[880] Ohne auf das abweichende Votum der Richter in der ersten Tagebuchentscheidung einzugehen, argumentierte der Senat erneut mit der Verpflichtung zur umfassenden Wahrheitsermittlung, die sich auf alle Merkmale erstrecke, die für die Beurteilung der strafrechtlichen Schuld und die Strafzumessung von Bedeutung seien.[881] Der zweite Senat trug dabei trotz Kenntnis des abweichenden Sondervotums des eigenen Senats aus dem Jahre 1989 und der Rechtsauffassung des ersten Senats aus dem Jahre 2004 nichts zu einer Vereinheitlichung der Rechtsprechung bei. Wünschenswert wäre wenigstens eine kritische Auseinandersetzung mit der differierenden Rechtsprechung gewesen.

(2.3) Neuere Rechtsprechung des BVerfG

Der erste Senat des BVerfG fasste im Jahre 2016 im Urteil zur Verfassungsmäßigkeit des Bundeskriminalamtsgesetzes die Rechtslage zum Straftatvorbehalt bei verkörperten Nachrichten sowie Gesprächen dem Grunde nach entsprechend der engeren Linie des ersten Senats aus der Entscheidung zum großen Lauschangriff zusammen. Zwar bleibt die höchstpersönliche Kommunikation unmittelbar über Straftaten nicht geschützt, da die Besprechung und Planung von Straftaten ihrem Inhalt nach Sozialbezug aufweise und folglich nicht zum Kernbereich privater Lebensgestaltung gehören könne.[882] Insoweit befindet sich der erste Senat noch auf der Rechtsprechungslinie des zweiten Senats aus der Tagebuchentscheidung, was er durch eine entsprechende Zitation der beschriebenen Urteile des zweiten Senats auch deutlich macht. Im Folgenden wird sodann aber ersichtlich, dass der Kernbereich dennoch unter keinem generellen Abwägungsvorbehalt zugunsten der öffentlichen Sicherheitsinteressen steht.[883] So sollen sowohl Aufzeichnungen als auch Äußerungen im Zwiegespräch, die beispielsweise innere Eindrücke und Gefühle ausdrücken aber keine Hinweise auf konkrete Straftaten enthalten, nicht schon dadurch dem Kernbereich entzogen sein, da sie die Ursachen oder Beweggründe eines

880 BVerfG, Beschluss vom 26. Juni 2008 – 2 BvR 219/08, Rn. 21 = BVerfGK 14, 20, 25.
881 BVerfG, Beschluss vom 26. Juni 2008 – 2 BvR 219/08, Rn. 21 = BVerfGK 14, 20, 25.
882 BVerfGE 109, 279, 319; BVerfGE 141, 220, Rn. 122; neulich ebenso BVerfG, NJW 2020, 2235, Rn. 202.
883 So auch BVerfG, NJW 2020, 2235, Rn. 202.

strafbaren Verhaltens offenbaren.[884] Die Konsequenz hieraus bleibt damit, dass höchstpersönliche Informationen in diesen Fällen auch dann als dem Kernbereich zugehörend betrachtet werden müssen, wenn sie für Aufklärung von Straftaten oder Gefahren hilfreiche Aufschlüsse geben könnten. Schließlich müsse es – so lange diese Gespräche nicht unmittelbar Straftaten zum Gegenstand haben – die Möglichkeit geben, sich Vertrauenspersonen zu offenbaren. Es müsse dem Einzelnen möglich bleiben, ein Fehlverhalten einzugestehen oder sich auf dessen Folgen einzurichten, wie dies etwa in Form eines Beichtgespräches oder vertraulichen Gespräche mit einem Psychotherapeuten oder einem Strafverteidiger erfolgen kann.[885] Diese höchstpersönliche Privatsphäre müsse dem Staat absolut entzogen bleiben.[886] Allerdings werden gerade diese Gespräche häufig sogar einen unmittelbaren Bezug zu Straftaten aufweisen. Entgegen der allgemeinen höchstrichterlichen Leitlinie, dass in einem solchen Fall der Kernbereich nicht eröffnet ist, wird für diese Fälle der Straftatvorbehalt praktisch ausgesetzt.[887] Dies ist zutreffend, schließlich würde der Mandant oder Patient seine sensiblen Informationen ansonsten nicht ohne Schutz vor staatlicher Überwachung offenbaren können. Nicht zuletzt hätte dies zur Folge, dass eine zielführende Strafverteidigung oder Psychotherapie nicht möglich wäre. Gerade im Falle der Strafverteidigung wäre dies wiederum nicht mit dem Rechtsstaatsprinzip und daran anknüpfend dem Recht des Betroffenen auf eine wirksame Strafverteidigung zu vereinbaren. In der nunmehr aktuellsten Entscheidung zum Straftatvorbehalt aus dem Jahr 2018 hielt sich der zweite Senat des BVerfG mit Ausführungen zum Unmittelbarkeitskriterium zurück. Lediglich pauschal wurde dargelegt, dass der Charakter und die Bedeutung des Inhalts entscheidend seien. Dabei sei ein unmittelbarer Bezug zu Straftaten gegeben, wenn Angaben über deren Planung oder Berichte über begangene Straftaten in Rede stehen.[888]

884 BVerfGE 141, 220, Rn. 122; BVerfG, NJW 2020, 2235, Rn. 202.
885 BVerfGE 141, 220, Rn. 122.
886 BVerfGE 141, 220, Rn. 122.
887 BVerfGE 141, 220, Rn. 122; *Reichert*, Der Schutz des Kernbereichs, S. 51.
888 BVerfG, Beschluss vom 18. April 2018 – 2 BvR 883/17 -, Rn. 28, mit Verweis jedoch ausschließlich auf die Entscheidung des 2. Senats vom 14. September 1989 in BVerfGE 80, 367.

(2.4) Auffassung Roxins

Einen abweichenden Weg zum Umgang mit dem Straftatvorbehalt schlägt *Roxin* vor, der hinsichtlich der Frage, ob ein Zwiegespräch über Straftaten einen Sozialbezug aufweist und daher aus dem Kernbereich herauszunehmen ist, danach differenzieren will, ob es sich um sachliche Deliktsbesprechungen unter Straftatbeteiligten bzw. Mitwissern handelt oder ein Straftäter beispielsweise unter Tränen seiner Ehefrau die Tat beichtet.[889] Im letzten Fall würde der Kernbereichsschutz bestehen bleiben.[890] Diesem von *Roxin* gegangenen Weg innerhalb eines Zwiegespräches zwischen der Art des Zwiegespräches zu differenzieren ist durchaus positiv zu beurteilen. So macht es in der Tat einen Unterschied, ob eine planvoll agierende Familienbande sich über vergangene oder zukünftige Verbrechen unterhält oder ein Ehepartner dem anderen in einer emotionalen Ausnahmesituation eine begangene Straftat gesteht. Während das Ganovengespräch über begangene Straftaten, einzig den Zweck verfolgt, vergangene Straftaten zu besprechen oder neue zu planen, tatsächlich mit einem Verfall der schützenswerten Persönlichkeit assoziiert werden kann, kann dies für die emotionalen Beichte nicht gelten. In dieser Situation geht es keineswegs um den Verfall der Persönlichkeit, sondern womöglich gar um deren Widerherstellung. Der mit der Beichte einhergehende Einblick in das tiefste Innere der Persönlichkeit des Betroffenen scheint prädestiniert für eine endgültige Zuordnung zum Kernbereich. Anders ist dies freilich, wenn der Betroffene seiner Ehefrau nüchtern von seinen in der Vergangenheit begangenen Straftat erzählt um, diese hierüber aufzuklären oder vor dieser mit den begangenen Taten zu prahlen.[891] Eine nüchterne, sachliche Bilanz in Form einer „sachlichen Deliktsbesprechung“[892] kann, gleich wie eng das zwischen den Personen stehende Vertrauensverhältnis auch sein mag, nicht zum absolut geschützten Kernbereich gehören. Dennoch wird angenommen, dass auch solche bloß berichtenden Äußerungen im Zwiegespräch zum Kernbereich zu zählen ist.[893] Diese Sichtweise vergisst allerdings den Kernzweck des Kernbereichsschutzes. Der höchstpersönliche Kernbereich will keinen Freischuss hinsichtlich jeglicher Art von Kommunikation erteilen, sondern diese vielmehr nur dann dem staatlichen Zu-

889 FS-Wolter/*Roxin*, 1057, 1069.
890 FS-Wolter/*Roxin*, 1057, 1069.
891 *Schwabenbauer*, Heimliche Grundrechtseingriffe, S. 268.
892 FS-Wolter/*Roxin*, 1057, 1069.
893 *Wolter*, StV 1990, 175, 179; *Fink*, Intimsphäre und Zeugenpflicht, S. 173, 178.

griff entziehen, wenn sich die Kommunikation als das Ergebnis menschlichen Verlangens nach Öffnung und dem Zeigen innerer Eindrücke und Gefühle darstellt. In dem Fall des nüchternen Besprechens einer Straftat steht nicht mehr die Verarbeitung der eigenen Gefühle als Teil der Selbstreflexion im Vordergrund, sondern die Straftat selbst.[894] Insofern könnte zu fragen sein, wie dieser Sichtweise folgend mit der Situation umzugehen wäre, in der der Täter seine Ehefrau unter Tränen gesteht, eine Straftat begehen zu wollen, um beispielsweise auch in Zukunft für die Familie sorgen zu können. Da der Täter die Straftat hier erst zu begehen plant, könnte dies nicht als vermeintlicher Akt der Wiederherstellung der verfallenen Persönlichkeit anzusehen sein. Womöglich ist also auch hinsichtlich des beichtenden Zwiegespräches zwischen vergangenen und zukünftigen geplanten Straftaten zu unterscheiden. Sofern allerdings durch das Geständnis gegenüber der Ehefrau zum Ausdruck gebracht wird, dass der Betroffene beispielsweise keinen anderen Ausweg sieht und sich nicht anders als durch die Begehung einer Straftat zu helfen weiß, muss konsequenterweise auch dieses Gespräch als Ausfluss der Verarbeitung eigener Empfindungen als dem Kernbereich zugehörend gewertet werden. Es kann sodann keinen Unterschied hinsichtlich der Verwertbarkeit erlangter Informationen machen, ob das aufgezeichnete Zwiegespräch vor oder nach der begangenen Straftat stattfand.

(3) Im Rahmen eines Selbstgespräches

(3.1) Die BGH-Rechtsprechung

Hingegen soll der vom Bundesverfassungsgericht vorgenommene Kernbereichsausschluss im Hinblick auf geäußerte Straftaten nicht auf ein abgehörtes Selbstgespräch übertragen werden können. Dies folgerte der BGH erstmals, als er im Jahr 2005 die Verwertbarkeit eines in einem Krankenzimmer aufgezeichneten Selbstgespräches mit den Worten: „*Sehr aggressiv, sehr aggressiv, sehr aggressiv! In Kopf hätt i eam schießen sollen, in Kopf hätt i eam schießen sollen, selber umgebracht … in Kopf hätt i eam schießen sollen*" von der Verwertbarkeit ausschloss, da es dem unantastbaren Kernbereich zuzurechnen sei.[895] Die durch das Bundesverfassungsgericht aufgestellte

894 Diesbezüglich zutreffend *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 92.

895 BGH, NJW 2005, 3295, 3296.

Regelvermutung, wonach bei einem Gespräch über Straftaten ein Sozialbezug gegeben sei, sei auf Selbstgespräche bereits nicht anwendbar, weil es sich dabei nicht um eine Kommunikation mit der Außenwelt, sondern um eine Selbstauseinandersetzung handle.[896] Einem Selbstgespräch fehle es nach den Ausführungen des Bundesgerichtshofes stets an einem Sozialbezug. Dies soll darauf gründen, dass die Rechtsprechung des BVerfG zum fehlenden Sozialbezug von vorn herein nur für die Fälle eines (Zwie-)Gespräches gelte, nicht jedoch für eine bloße Äußerung im Rahmen eines Selbstgespräches.[897] Bei einem Selbstgespräch trete die Eindimensionalität der ablaufenden Kommunikation, die Nichtöffentlichkeit, die mögliche Unbewusstheit der Äußerungen im Selbstgespräch, die Identität der Äußerung mit den inneren Gedanken und „die Flüchtigkeit des gesprochenen Wortes“ in den Vordergrund.[898] Das Strafverfolgungsinteresse müsse dann zurücktreten.[899] Diese Rechtsprechung behielt der BGH auch in seiner zweiten Entscheidung zur Verwertbarkeit eines Selbstgespräches bei. Dieser Entscheidung aus dem Jahr 2011 lag die Frage nach der Verwertbarkeit eines in einem PKW aufgezeichneten Selbstgespräches zugrunde. An die Entscheidung aus dem Jahr 2005 anknüpfend zählte der Bundesgerichtshof das „laute Denken" zur Existenzbedingung des Menschen, womit dieses Verhalten stets dem Kernbereich unterfallen müsse.[900] Exemplarisch zeigte das Gericht die aus seiner Sicht entscheidenden Unterschiede zur ergangenen Rechtsprechung hinsichtlich Tagebuchaufzeichnungen und Zwiegesprächen auf. Während in der Tagebuchentscheidung die Flüchtigkeit des gesprochenen Wortes nicht von Bedeutung war, da der Betroffene seine Gedanken in einem Tagebuch fixiert hatte, erlangt die Flüchtigkeit des gesprochenen Wortes als Abgrenzungskriterium im Falle eines Selbstgespräches besonderes Gewicht. Ferner hätten in der Tagebuchentscheidung des BVerfG auch präventive Überlegungen der Annahme der Verwertbarkeit zugrunde gelegen, weil die dortigen Tagebuchaufzeichnungen

896 *Wolter* in: SK-StPO, § 100c StPO, Rn. 63; *Gercke* in: HK-StPO, § 100f StPO, Rn. 12; FS-Wolter/*Roxin*, 1057, 1070 ff.; FS-Geppert/*Roxin*, 549, 565.

897 BGH, NJW 2005, 3295, 3297; zweifelnd *Reichert*, Der Schutz des Kernbereichs, S. 54; *Barrot*, Der Kernbereich, S. 119 f.

898 BGHSt 57, 71, 75.; *Zabel*, ZJS 2012, 563, 565; als Fünf-Kriterien-Prüfprogramm bezeichnend *Jahn/Geck*, JZ 2012, 561, 564; kritisch hinsichtlich dieser Kriterien *Wohlers*, JR 2012, 389.

899 BGH, NJW 2005, 3295, 3296; *Mitsch*, NJW 2012, 1486, 1488; *Deiters/Albrecht*, ZJS 2008, 319, 322.

900 BGHSt 57, 71, 75, Rn. 15; zustimmend *Mitsch*, NJW 2012, 1486, 1488; *Muthorst*, StudZR 2013, 169, 174.

vor der Tatbegehung gemacht worden waren und so im Rahmen der Gefahrenabwehr auch zur Verhinderung der Tat hätten genutzt werden können.[901] Dagegen spiele die Möglichkeit der Prävention zu Gunsten anderer Grundrechtsträger im Falle einer bereits begangenen Straftat keine Rolle. Es komme daher nicht zu einer Grundrechtskollision, die durch eine Abwägung aufzulösen wäre.[902] Zudem kann das Selbstgespräch auch deshalb nicht mit einem Zwiegespräch gleichgesetzt werden, da die Äußerungen in einem Selbstgespräch gerade nicht auf Verständlichkeit angelegt sind und zudem durch unwillkürlich auftretende Bewusstseinsinhalte gekennzeichnet seien.[903] Im Gesamten sei der Inhalt der Gedankenäußerung bei Selbstgesprächen im Unterschied zur Fixierung von Gedanken in einem Tagebuch oder eines Gesprächs mit Dritten – überhaupt nicht mehr entscheidend.[904]

(3.2) Kritik

Diese Rechtsprechungslinie sah sich deutlicher Kritik der Literatur ausgesetzt. Aus § 100c Abs. 4 S. 3 StPO a.F. ergebe sich, dass Gespräche über begangene Straftaten nicht dem Kernbereich angehören könnten, unabhängig um was für eine Art von Gespräch es sich dabei handle.[905] Ferner enthalte § 100c Abs. 4 S. 3 StPO a.F. auch keine Anhaltspunkte für die von der höchstrichterlichen Rechtsprechung vorgenommenen Differenzierung zwischen „Äußerung" im Sinne eines Selbstgespräches und „Gespräch" im Sinne eines Zwiegespräches.[906] Fraglich ist darüber hinaus, ob die Ausführungen des Bundesverfassungsgerichts tatsächlich, wie vom Bundesgerichtshof angenommen, eine inhaltliche Differenzierung zwischen Selbst-

901 BGHSt 57, 71, 76 f., Rn. 17.
902 BGHSt 57, 71, 76 f., Rn. 17.
903 BGHSt 57, 71, 77, Rn. 18.
904 BGHSt 57, 71, 75, Rn. 15 f.; zustimmend *Eisenberg*, Beweisrecht StPO, Rn. 2527a; *Lindemann/Reichling*, StV 2005, 650, 652; *Ellbogen*, NStZ *2006, 180; Zabel, ZJS 2012, 563, 565; Habetha, ZWH 2012, 165; von Heintschel-Heinegg, JA 2012, 395, 396; Ladiges, StV 2012, 517; Mitsch, NJW 2012, 1486, 1488; Wohlers, JR 2012, 389; Valerius, JA 2006, 15, 16; Jahn, JuS 2006, 91, 92; ders. StraFo 2011, 117, 119; Renka*, Verwertbarkeit von Selbstkommunikation, *S. 191; Dalakouras*, Beweisverbote und Intimsphäre, S. 265*; ablehnend vor allem Warg, NStZ 2012, 237, 240; im Ergebnis auch Fleischmann, NJ 2012, 218 f.*
905 Fezer-FS/*Rogall*, S. 61, 70.
906 *Warg*, NStZ 2012, 237, 240; *Zimmermann*, GA 2013, 162, 172 f.; *Löffelmann*, ZIS 2006, 87, 92.

und Zwiegespräch beinhalten sollten. In der Entscheidung zum großen Lauschangriff habe das Verfassungsgericht schließlich durch die Formulierung *„wenn sich jemand allein oder ausschließlich mit Personen in der Wohnung aufhält […] und es keine konkreten Anhaltspunkte gibt, dass die zu erwartenden Gespräche nach ihrem Inhalt einen unmittelbaren Bezug zu Straftaten aufweisen*“[907], zum Ausdruck gebracht, dass die Terminologie „Gespräch“ im Lichte der Entscheidung auch dann zutreffend sei, wenn ein bloßes Selbstgespräch stattfinde. Dies sei daraus zu schließen, dass das Gericht die beiden Fälle eines Zwiegesprächs und eines Selbstgesprächs in einem Satz zusammenfasste und im Folgenden als Gespräch einordnete.[908] Da das Bundesverfassungsgericht zur Verwertbarkeit von Selbstgesprächen bislang ausdrücklich keine von der Tagebuch-Judikatur abweichenden Maßstäbe formulierte, sei anzunehmen, dass diese auf die übrigen Fälle mit Kernbereichsrelevanz zu übertragen sind.[909] Hinzu komme die Intension des Gesetzgebers, der zwar die Vermutung aufstellte, dass Selbstgespräche in der Regel in den absolut geschützten Kernbereich fallen werden, jedoch gerade nicht die Aussage traf, dass solche Selbstgespräche niemals einen Sozialbezug aufweisen können.[910] Es sei daher mit der Rechtssicherheit nicht zu vereinbaren nichtöffentliche Selbstgespräche ausnahmslos dem Kernbereich zuzuordnen. Vielmehr sei der Straftatvorbehalt auch auf Selbstgespräche zu erstrecken.[911]

(3.3) Einschränkung auf beichtende Selbstgespräche

Ferner wird vorgeschlagen lediglich das „sachlich berichtende“ Selbstgespräch aus dem Kernbereich auszunehmen.[912] Dies begründet *Rottmeier* mit dem Ziel einer einheitlichen Kernbereichsbestimmung sowohl für Tagebucheinträge, Zwie- als auch Selbstgespräche. Anhand dessen, ob der Schwerpunkt des Selbstgesprächs einen selbstreflektierenden oder berichtenden Charakter besitze, könne sodann losgelöst von der formalen Sonderdogmatik des BGH entschieden werden, ob das Selbstgespräch tatsäch-

907 BVerfGE 109, 279, 319.
908 *Kolz*, NJW 2005, 3248, 3249; *Traub*, Verwertbarkeit von Selbstgesprächen, S. 83.
909 *Allgayer*, NStZ 2012, 399.
910 Fezer-FS/*Rogall,* S. 61, 70; *Löffelmann*, ZIS 2006, 87, 92.
911 *Zimmermann*, GA 2013, 162, 173; *Haverkamp*, Jura 2010, 492, 495.
912 *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 93.

lich noch dem Kernbereich zuzuordnen ist.[913] Dem Bestreben nach Vereinheitlichung ist zwar grundsätzlich zuzustimmen, im Falle der Selbstgespräche, sind diese aufgrund ihres speziellen Charakters jedoch symptomatisch für die Einschlägigkeit des höchstpersönlichen Kernbereichs. Das Selbstgespräch als „kleiner Bruder" des stillen Denkens muss stets – unabhängig seines Inhalts – dem Kernbereich zugeordnet werden. Hieraus gewonnene Informationen dürfen nicht auf repressiver Ebene gegen den Betroffenen verwendet werden. Das laute Denken zum Gegenstand eines Strafprozesses zu machen, darf genauso wenig der Fall sein, wie mittels moderner Technik versucht werden darf, in die Gedankenwelt des Betroffenen einzudringen.[914] Zu nahe liegen stilles und lautes Denken in Form eines Selbstgespräches – an einem Ort, der zudem unter der vollständigen Beherrschbarkeit des Betroffenen steht – beisammen. Im Übrigen darf der Drang nach Vereinheitlichung nicht dazu führen, letztlich ungleiches nach gleichen Maßstäben zu behandeln. Für eine umfassende Zuordnung jedenfalls des Selbstgespräches zum Kernbereich spricht zuletzt auch, dass der Gesetzgeber im Rahmen der Neufassung des § 100d StPO auf einen Straftatvorbehalt verzichtete. In § 100d StPO – als Nachfolger des früheren § 100c StPO a.F. – wurde der die entsprechende Vorschrift enthaltene Satz 3 aus § 100c Abs. 4 StPO a.F. nicht übernommen. Die Frage nach der Betroffenheit des Kernbereichs soll, auf Grund tatsächlicher Anhaltspunkte jeweils konkret unter Berücksichtigung aller Umstände des Einzelfalles ermittelt werden.[915] Dies muss als Abkehr des Gesetzgebers davon verstanden werden, bei sämtlichen Gesprächen über Straftaten von einem generellen Kernbereichsausschluss auszugehen.

2) Stellungnahme

a) Allgemeines

Es ist unumstößlich, dass ein Bereich existieren muss, der dem staatlichen Zugriff entzogen ist. Die Daseinsberechtigung eines solchen „Kernbereiches höchstpersönlicher Lebensgestaltung" kann nicht in Zweifel gezogen werden. Entscheidend bleibt dessen inhaltliche Ausgestaltung. Die Indi-

913 *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 93 f.
914 FS-Wolter/*Roxin*, 1057, 1070.
915 BT-Drs. 18/12785, S. 57.

katoren, die maßgeblich auf Ebene der Beweiserhebung zum Vorschein treten, stellen dabei eine Art „äußere Hülle" der Höchstpersönlichkeit dar. Aus der Rechtsprechung lässt sich derweil folgern, dass vor allem auf den gesprochenen Inhalt zur Einordnung abgestellt wird. Mit dieser Situation geht ein vergleichsweiser großer Spielraum einher, der den Gerichten bei der Frage nach der Verwertbarkeit einer Information zukommt. Während dies unter dem vermeintlichen Deckmantel einer möglichst hohen Einzelfallgerechtigkeit im Lichte des konkreten Falles für positiv empfunden werden könnte, stellt sich dennoch die Frage, ob dies den Maßstäben an ein faires Strafverfahren noch genügen kann.[916] Naturgemäß kann mittels des Gesprächsinhalts am zielgenauesten eine Gesprächszuordnung zum höchstpersönlichen Lebensbereich erfolgen. Gleichwohl bleibt die Definition, wann der Gesprächsinhalt als ein den Kernbereichsschutz auslösender höchstpersönlicher Inhalt einzuordnen ist, überaus vage. In der Rechtsprechung des Bundesverfassungsgerichts wird das Inhaltskriterium in verschiedenen Formen umschrieben. So seien hiervon das zum Ausdruck bringen *„innerer Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art"* oder auch *„Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität"* erfasst.[917] Demnach lassen sich verschiedene Fallgruppen als Akt höchstpersönlicher Natur herausarbeiten. Hierzu zählen beispielsweise Reflexionen des Verfassers über seine Persönlichkeitsstruktur, wie etwa über seine Gefühle, Sehnsüchte, Sympathien- und Antipathien, Glücksmomente, Wünsche, Fehler, Schwächen, Ängste, Nöte, Zwänge, Triebe oder Spannungen. Daneben kommen als Bezugspunkte der enge Familienkreis, enge Freundschafts- und Liebesverhältnisse, schwere Krankheiten, Sexualität und Religion in Betracht.[918] Insofern ist zwar korrekt, dass durchaus eine Umschreibung des Höchstpersönlichen vorgenommen werden kann und so eine Grenzziehung zwischen Kernbereich und Privatsphäre möglich erscheint. In der praktischen Umsetzung darf jedoch bezweifelt werden, ob dies zu eindeutigen Ergebnissen führt. Die oben dargelegte Stimmengleichheit im zweiten Senat des Bundesverfassungsgerichts hinsichtlich der Zuordnung eines Sachverhalts zum höchstpersönlichen Kernbereich stammt zwar bereits aus dem Jahr 1989, mithin aus einer Zeit vor der Entscheidung zum Lauschangriff aus dem Jahr 2004, in welcher das Kriterium der Höchstpersönlichkeit erstmals näher beleuchtet

916 ähnlich *Berkemann*, JR 1990, 226, 227.
917 BVerfGE 109, 279, 313.
918 Vgl. die Beispiele bei *Ellbogen*, NStZ 2001, 460, 463.

wurde. Dennoch zeigt die Argumentation der Verfassungsrichter aus dem Jahr 1989, dass sich diese im Kern bereits mit den gleichen Fragen zur Höchstpersönlichkeit wie auch die Richter im Jahr 2004 beschäftigten. So argumentierten die Richter der nicht tragenden Entscheidung mit der Wiedergabe bestimmter Gemütszustände, Reflexionen über die eigene Persönlichkeitsstruktur, der schonungslosen Darstellung seiner Gefühlswelt und quälenden Problemen des Betroffenen, mit welchen dieser ins Reine kommen wollte.[919] Dies zugrunde gelegt wäre bereits die 1989 ergangene Tagebuchentscheidung überaus geeinigt gewesen, unter Beweis zu stellen, dass es sich bei dem höchstpersönlichen Kernbereichs nicht lediglich um ein auf seltenste Einzelfälle beschränktes Konstrukt handelt. Stattdessen gewinnt man den Eindruck, dass die Gerichte darauf bedacht sind, der Konsequenz zu entgehen, einen abgrenzbaren Kernbereich zu erhalten, der in letzter Konsequenz sodann auch in Fällen schwerster Kriminalität zu einem Beweismittelverlust führen könnte. Hiermit steht in Einklang, dass in der höchstrichterlichen Rechtsprechung bislang in keinem Fall angenommen wurde, dass beispielsweise tagebuchartige Aufzeichnungen dem unantastbaren Kernbereich angehören. Vielmehr kommt es in der BGH-Rechtsprechung unmittelbar zu einer Interessensabwägung, die sodann in Fällen der Schwerstkriminalität zwangsläufig zu einer Bejahung der Verwertbarkeit führen wird.[920] Dies geht teilweise gar soweit, dass alleine aufgrund des Vorliegens einer der „schwersten Straftaten" der persönlichkeitsrelevante Hintergrund der Aufzeichnung keiner Würdigung mehr unterzogen wird, sondern schlicht mit dem Überwiegen der Interessen der Strafrechtspflege eine Verwertbarkeit etwaiger Aufzeichnungen bejaht wird.[921]

Es muss um den Schutz des Kernbereichs willen daher einer Linie gefolgt werden, die garantiert, dass das Ergebnis eines für den Beschuldigten massive Einschnitte mit sich bringende Strafverfahrens nicht von der Besetzung des Senats und den persönlichen Wertungen der Richter abhängig ist. Hierfür muss eine mutigere Zuordnung eines hierfür qualifizierten Sachverhalts zum persönlichen Kernbereich erfolgen und sodann konsequent auf jegliche weitere Abwägung verzichtet werden. Korrespondierend hiermit ist in ausnahmslos allen Selbstgesprächen, welche der Betroffene in einer abgeschlossenen Räumlichkeit in dem Gefühl von Abgeschiedenheit führt, ein mit Geheimhaltungswillen vorgenommener

919 BVerfGE 80, 367, 381 (abw. Meinung).
920 *Ellbogen*, NStZ 2001, 460, 463.
921 Vgl. BGHSt 34, 397, 401.

höchstpersönlicher Akt zu sehen. Daneben sind Zwiegespräche nicht ausnahmslos dem Kernbereich zuzuordnen, sondern müssen in Anbetracht der Umstände des Einzelfalls untersucht werden. Zuvörderst ist dabei die Thematik der Kommunikation zu beurteilen, zu der jedoch, um von einer Kernbereichsbetroffenheit ausgehen zu können, weitere typische Merkmal hinzutreten müssen. Das entsprechende Gespräch müsste an einem Ort geführt werden, der dem Herrschaftsbereich des Betroffenen zuordnen ist oder es müsste sich aus objektivierbaren Kriterien ein Vertrauensverhältnis zwischen den Kommunizierenden Personen herleiten lassen. Eine jahrelange Freundschaft oder eine partnerschaftliche Beziehung deuten in diesem Zusammenhang auf ein erhöhtes Vertrauensverhältnis hin. Ein solches wird nicht zu Bekannten des letzten Kneipenbesuches oder Personen, zu denen nur ein sporadischer Kontakt gepflegt wird, bestehen. Die Anzahl, der in ein Gespräch verwickelten Personen, ist lediglich als subsidiäres Indiz einzuordnen. Jedenfalls so lange die Anzahl der Personen für den Betroffenen überschaubar ist und zu diesen ein enges Vertrauensverhältnis besteht, spricht auch eine höhere Anzahl involvierter Personen nicht gegen eine Kernbereichsrelevanz.

b) Der Sozialbezug

Ferner muss hinsichtlich des von einem Straftatengespräch ausgehenden Sozialbezug differenziert werden. Ein unmittelbarer Sozialbezug der unumstößlich zum Ausschluss des Kernbereichs führt, kann nur in einer solchen Situation vorliegen, in der die Überwachung des Betroffenen unmittelbar eine verübte Straftat offenbart. Diese Straftat betrifft in diesen Fällen unmittelbar die Selbstbestimmungsfreiheit Dritter und weist sodann einen unmittelbaren Sozialbezug auf. Im Falle der Vergewaltigung beispielsweise mag das sexuelle Bedürfnis des Täters zwar ein innerstes Empfinden sein, sofern durch die Aufzeichnung dagegen unmittelbar der Ablauf der Tat nachvollzogen wird, besteht zum Zeitpunkt der Aufzeichnung ein unmittelbarer Sozialbezug. Dieser Sozialbezug ist durch das Kriterium der Unmittelbarkeit der Straftat, die mit der „Live-Überwachung" der Tat einhergeht, auch wesentlich höher einzuordnen als der Sozialbezug eines Selbstgespräches oder einer Tagebuchaufzeichnung über die gleiche, in der Vergangenheit liegende, Tat.[922] Entscheidend für das Vorliegen des Sozialbezuges ist daher nicht, ob ein solcher besteht, sondern von welcher Art

922 Vgl. auch *Metz*, NStZ 2020, 9, 10.

und Intensität dieser ist.[923] Insoweit ist dem durch das Bundesverfassungsgericht im ersten Tagebuchurteil aufgestellten Maßstab zu folgen. Bei Tagebucheinträgen oder Selbstgesprächen lässt sich sodann aber kein derartiger Sozialbezug herleiten, der den Kernbereichsschutz pauschal entfallen ließe, da allein die Existenz oder der Inhalt einer Tagebuchaufzeichnung oder eines Selbstgespräches die Sphäre Dritter gerade nicht berührt.[924]

c) Umgang mit einem Selbstgespräch

Hinsichtlich eines Selbstgespräches kann – im Übrigen auch nach alter Rechtslage – nur eine pauschale, abwägungsresistente Zuordnung zum Kernbereich, dass einem Selbstgespräch anhaftende „Mehr" im Vergleich zu einem Zwiegespräch verdeutlichen. Es stellt freilich nochmals einen Unterschied dar, ob der Betroffene das Zwiegespräch sucht und damit Informationen seiner Kontrolle preisgibt oder dieses nur mit sich selbst führt. Hinzu kommt, dass die nach zutreffender Ansicht bestehende Möglichkeit nach § 100c StPO auf einen Smart Speaker zuzugreifen mit einem weiter fortschreitenden Kontrollverlust des Betroffenen hinsichtlich seiner eigenen Wohnung einhergeht. Während der Wohnungsbesitzer seine eigene Wohnung theoretisch permanent videoüberwachen könnte, um mögliche Eindringlinge (auch Ermittlungsbeamte beim Anbringen der Wanzen) zu entdecken, ist dem Betroffenen diese Möglichkeit beim „Anzapfen" eines Endgerätes (Smart Speaker) genommen. Umso wichtiger ist daher, dass diesem in dem Gefühl vollkommener Abgeschiedenheit ein „letztes Refugium"[925] ohne staatlichen Zugriff verbleibt und er an diesem Ort seinen Gedanken freien Lauf lassen kann.

Auch wenn die Kritik an der pauschalen Zuordnung eines Selbstgesprächs zum Kernbereich angesichts dessen, dass so im „worst case" eine erhebliche Straftat nicht abgeurteilt werden könnte, eine vor allem moralische Berechtigung erfahren mag, so ist der konsequenten und ausnahmslosen Rechtsprechung des Bundesgerichtshofs in Anbetracht der unantastbaren Menschenwürde dennoch zuzustimmen. Die unterschiedlichen Schutzwürdigkeit von im Zwie- oder im Selbstgespräch geäußerten Informationen ist unmittelbar aus der Menschenwürde ableitbar. Bei einem nichtöffentlichen Selbstgespräch handelt es sich um das Aussprechen inne-

923 BVerfGE 80, 367, 374.
924 Zutreffend *Kleb-Braun*, CR 1990, 344, 346, *Ellbogen*, NStZ 2001, 460, 463.
925 BVerfGE 109, 279, 314.

rer Gedankenvorgänge zur eigenen, zurückgezogenen Verarbeitung des Erlebten und nicht zwecks Mitteilung an eine dritte Person. Dieser unterschiedliche Umgang des Betroffenen mit Informationen aus seinem Innersten darf auch im Strafverfahren nicht unberücksichtigt bleiben.[926] Ob bewusst oder unbewusst entscheidet sich der Täter gerade nicht für ein Zwiegespräch oder das Niederschreiben seiner Gedanken, die er daher offensichtlich nicht einmal manifestiert wissen möchte. Auch anhand einer stringenten Subsumtion unter der gerichtlichen Voraussetzung der Gemeinschaftsbezogenheit bleibt es bei der Unverwertbarkeit eines Selbstgespräches. Ebenso wie Gedanken im Inneren verbleiben und folglich keine Gemeinschaftsbezogenheit aufweisen, gilt dies aufgrund des zu diesen Gedanken bestehenden untrennbaren Zusammenhangs auch für das laute Denken in Form eines Selbstgespräches. Dieses ist ebenso wenig an einen Kommunikationspartner gerichtet sondern als laute Äußerung bloßer Gedanken dem Kernbereich zuzuordnen. Daher ist das Selbstgespräch auf einer noch höheren Stufe der Schutzwürdigkeit anzusiedeln als das Zwiegespräch oder der Tagebucheintrag. Die aus einem Selbstgespräch an einem besonders geschützten Ort gewonnenen Inhalte sind weder als solche noch als sog. Spurenansatz im Prozess zuzulassen. Dies stellt mithin einen rechtsstaatlich gangbaren Mittelweg dar, der lautes Denken und eine effektive Strafverfolgung versucht zu vereinbaren.[927] Dieses Ergebnis bleibt auch dann unberührt, wenn man sich die Frage stellt, ob das Selbstgespräch im Beisein eines Smart Speakers mithin in einer zunehmend digital erfassten Welt noch als solches angesehen werden kann und ob der Betroffene in diesem Zusammenhang tatsächlich noch auf die Flüchtigkeit des gesprochenen Wortes vertrauen kann.[928] Allein die abstrakte Möglichkeit, dass sich der Betroffene gemeinsam mit einem informationstechnischen System in einer Räumlichkeit aufhält, kann nicht dazu führen, dass dem Selbstgespräch die Vertraulichkeit und darauffolgend die Schutzwürdigkeit abzusprechen ist. Auch in einer zunehmend digitalisierten Welt ist ein informationstechnologisches System vor dem Hintergrund dessen eigentlicher Zwecksetzung und Aufgabenzuordnung nicht als „anwesende zweite Person" einzuordnen, die dem Selbstgespräch dessen Charakter als absolut schutzwürdig zu nehmen vermöge. Das verfassungsrechtlich statuierte Recht des Bürgers sich private Rückzugsräume zu erhalten, gilt unabhängig davon, ob in diesen auch digitalisierte Systeme integriert sind.

926 *Hohmann-Dennhardt*, NJW 2006, 545, 546.
927 So auch *Mitsch*, NJW 2012, 1486, 1488; *Wohlers*, JR 2012, 389, 390.
928 Zweifelnd *Gless*, StV 2018, 671, 677.

Dabei kann die Frage gestellt werden, ob diese abwägungsresistente Zuordnung auch für Konstellationen gelten muss, in denen der „Gesprächspartner" – beispielsweise ein Kleinkind oder eine komatöse Patientin – nicht in der Lage ist, am Gespräch teilzunehmen. Auf den ersten Blick würde man in einer solchen Konstellation ein Zwiegespräch erblicken, weshalb nicht die für ein Selbstgespräch geltenden Maßstäbe herangezogen werden dürften. Angesichts dessen, dass ein Kleinkind jedoch nicht aktiv am Gespräch teilnehmen kann und der Betroffene die physische Anwesenheit dieser Person womöglich zum „Selbstgespräch" nutzt, könnte gleichwohl ein Abstellen auf den Grundsatz abwägungsfreien Zuordnung eines Selbstgesprächs zum Kernbereich zu erwägen sein. Entscheidend und gleichfalls problematisch wäre dann allerdings, wann die an eine solche Person gerichtete Kommunikation aufgrund der besonderen Umstände noch als „Selbstgespräch" eingeordnet werden könnte und wann von einem Zwiegespräch ausgegangen werden müsste. Es müsste beispielsweise beurteilt werden, in welchen Fällen der „Gesprächspartner" als Kleinkind anzusehen wäre, sodass die Aussagen des Betroffenen noch als Selbstgespräch einzuordnen wären. Ein Abstellen auf das Alter des Kindes ist an dieser Stelle nicht zielführend. Weder ein Orientieren an der Deliktsfähigkeit des § 828 Abs. 1 BGB (7 Jahre), noch an der Strafmündigkeit des § 19 StGB (14 Jahre) können eine generelle Regelung bilden. Auf das Alter des Kindes rekurrierend, wäre ohnehin nicht ein pauschales Alter, sondern die Einsichtsfähigkeit des Kleinkindes im konkreten Fall, welche bekanntermaßen je nach Einzelfall erheblich divergieren kann, maßgeblich. In Anbetracht des umfassenden Schutzes eines Selbstgespräches – selbst, wenn dies erhebliche Straftaten zum Gegenstand hat – darf der unter ein solches Selbstgespräch fallende Sachverhalt, nicht zuletzt aus Verhältnismäßigkeitserwägungen, nicht zu sehr ausgeweitet werden. Wenn der Betroffene sein scheinbares Selbstgespräch in Gegenwart eines menschlichen Individuums führt, muss ihm stets bewusst sein, dass sein Gegenüber – selbst wenn dieser nach Auffassung des Betroffenen dazu subjektiv gar nicht in der Lage ist – einzelne Gesprächsfetzen auffasst und vor anderen Personen erneut von sich gibt. So hört man beispielsweise hin und wieder bezüglich komatöser Personen, dass diese ihr Umfeld durchaus wahrnehmen und verstehen können. Aufgrund der zweiten vorhandenen Person befindet sich der Betroffene in einer Situation, in der er nicht mehr vollkommen zurückgezogen, nur für sich ist. Die engen, aber notwendigen Voraussetzungen für die Annahme eines echten Selbstgespräches sind dann nicht mehr gegeben. Anders kann dies lediglich sein, wenn der „Gesprächspartner" nach festen wissenschaftlichen Erkenntnis-

sen nicht in der Lage ist eine Information aufzunehmen oder widerzugeben, wobei beispielsweise an Tiere oder Tote zu denken wäre. In allen anderen Fällen muss auf die für ein Zwiegespräch geltenden Grundsätze abgestellt werden.

d) Umgang mit einem Zwiegespräch

Ferner darf es aber auch bei konkreten Hinweise auf Straftaten innerhalb eines Zwiegesprächs oder einer Tagebuchaufzeichnung keinen pauschalen Kernbereichsausschluss geben. Zwar führen in diesen Konstellationen unmittelbare und konkrete Anhaltspunkte zu Straftaten zu einem weniger schützenswerten Gesprächsinhalt. Gleichwohl kann dieser Umstand nicht ausschließen, dass es sich dabei um einen Höchstpersönlichen Akt handelt, der dem Kernbereich zuzuordnen ist.[929] Insofern würde es sich anbieten, dass auch sofern in einem Tagebucheintrag oder einem Gespräch ein Bezug zu Straftaten besteht unterschieden wird, ob das ablaufende Gespräch oder die Aufzeichnungen einen nüchtern berichtenden bzw. planenden oder einen beichtenden Schwerpunkt besitzen. Schließlich wird nur der Beichtende eine Situation schaffen, die tiefere Rückschlüsse auf seine Persönlichkeit zulässt und damit die Basis für eine Zugehörigkeit zum höchstpersönlichen Kernbereich legt. Für eine solche Differenzierung streitet insbesondere, dass der Mensch – wie auch das Bundesverfassungsgericht fortlaufend betont – notwendigerweise in sozialen Bezügen existiere.[930] Dies ernstnehmend muss sodann dem menschlichen Individuum auch ein Bereich zuerkannt werden, in welchem er diesen sozialen Bezug ohne staatliche Überwachung in der Kommunikation mit anderen Individuen ausleben kann. Würde dem Individuum dieser Bereich genommen, sofern ein konkreter Bezug zu Straftaten bestünde, würde verkannt, dass gerade auch Straftaten die Persönlichkeit des Täters erheblich belasten können und das daher gerade in solchen Situationen die Möglichkeit der Interaktion in sozialen Bezügen mit einer weiteren Person existieren muss. Dem Bürger diesen Bereich ohne Beachtung der Intension eines

929 Vgl. auch *Küpper*, JZ 1990, 416, 420, der sich dafür ausspricht, die Schwere einer Straftat erst im Rahmen der Abwägung zu berücksichtigen, in die freilich erst dann eingetreten werden kann, wenn der eigentliche Gesprächsinhalt nicht dem Kernbereich zugehörend ist; a.A.: *Jäger*, GA *2008*, *473*, *491*.

930 BVerfGE 80, 367, 374; BVerfGE 109, 279, 319; BVerfGE 125, 175, 223; BVerfGE 132, 134, Rn. 64.

Zwiegespräches pauschal bei jeglichem konkreten Straftatenbezug zu nehmen, würde die verfassungsrechtliche garantierte Existenz des Menschen in sozialen Bezügen einseitig zugunsten des staatlichen Strafverfolgungsinteresses opfern. Anders ausgedrückt würde dieses Verständnis den Straftatvorbehalt als absolutes Ausschlusskriterium gegen die Zuordnung zum höchstpersönlichen Kernbereich verstehen und dem zugrunde legen, dass die Verfassung das Staatsverfolgungsinteresse stets höher gewichtet als das Recht des einzelnen in einem engen Kreis in sozialen Bezügen existieren zu dürfen. Ein solches generelles Überwiegen des staatlichen Sicherheitsinteresses gegenüber der aus Menschenwürdegarantie folgenden „Existenz in sozialen Bezügen" ist der Verfassung jedoch nicht einmal im Ansatz zu entnehmen. Der Differenzierung in beichtende sowie nüchtern berichtende Gespräche oder Aufzeichnungen kann auch nicht das Argument etwaiger Zuordnungsprobleme entgegengehalten werden. Zum einen folgt aus dieser Differenzierung bereits eine Vereinfachung der bestehenden Zuordnungsproblematik. Bei sämtlichen Zwiegesprächen oder Tagebucheinträgen müsste lediglich der typusprägende Charakter bestimmt werden, wohingegen weder eine Abgrenzung zwischen „konkreten Anhaltspunkten für Straftaten" und lediglich „mittelbaren Neigungen, die auf eine Straftat hindeuten" noch eine schwammige Zuordnung zur Höchstpersönlichkeit vorgenommen werden müsste, da einer beichtenden Erzählung über Straftaten dieser Punkt stets immanent wäre. Zudem stellen die zu präferierenden Kriterien solche dar, die zum einen subjektiv geprägt sind, zum anderen aber auch objektivierbar sind, wodurch ein Gespräch oder eine Aufzeichnung – auch für einen psychologischen Laien – eindeutig zuzuordnen sein wird.

e) Zusammenfassung

Nach alledem ist die unterschiedliche Behandlung eines Selbstgesprächs im Vergleich zu Zwiegesprächen oder Tagebuchaufzeichnungen gerechtfertigt. Dadurch wird zum einen der absoluten Schutzwürdigkeit des Selbstgespräches als Kopie der Gedanken Rechnung getragen und zum anderen anerkannt, dass Zwiegespräche aufgrund der Interaktion mit Dritten und Tagebuchaufzeichnungen aufgrund der Manifestation der Gedanken nicht auf der gleichen Ebene der Schutzwürdigkeit anzusiedeln sind und mithin nicht ausnahmslos dem Kernbereich zugeordnet werden können. Die Differenzierung zwischen beichtenden / reflektierenden und nüchtern berichtenden Zwiegesprächen und Tagebuchaufzeichnungen ge-

währleistet hingegen, dass der Kernbereich bei solchen hochpersönlichen Vorgängen nicht zur inhaltsleeren Hülle verkommt.

Für die Strafverfolgungsbehörden bedeutet dies, dass sofern es zu einem solchen (Beicht-)Gespräch kommen wird, die Beweiserhebung auch hinsichtlich eines Zwiegespräches unzulässig ist. Da es in den meisten Fällen an einer solchen Kenntnis fehlen wird, spricht im Sinne eines umfassenden Schutzes der Menschenwürde eine Vermutung dafür, dass alle Gespräche, die der Betroffene mit seinen engsten Vertrauten in der Wohnung führt zum Kernbereich privater Lebensgestaltung zu zählen sind.[931] In diesem Sinne müssen die Strafverfolgungsbehörde daher entsprechende konkrete Anhaltspunkte vorlegen, (beispielsweise durch die Kenntnis, dass die Familienbande zur Besprechung möglicher Straftaten zusammenkommt), um eine negative Kernbereichsprognose zu stellen und mithin eine rechtmäßige Beweiserhebung vornehmen zu können.[932] Die durch dieses Verständnis geschaffene Kernbereichsgarantie nimmt die dissentierenden Meinungen der Richterinnen Jaeger und Hohmann-Dennhardt im Rahmen des Urteils zum Großen Lauschangriff ernst, welche in ihrer abweichenden Meinung zum Urteil des ersten Senats des Bundesverfassungsgerichts zutreffend formulierten: *„wenn aber selbst die persönliche Intimsphäre, manifestiert in den eigenen vier Wänden, kein Tabu mehr ist, vor dem das Sicherheitsbedürfnis Halt zu machen hat, stellt sich auch verfassungsrechtlich die Frage, ob das Menschenbild, das solche Vorgehensweise erzeugt, noch einer freiheitlich-rechtsstaatlichen Demokratie entspricht“*.[933]

3) Umgang mit Mischgesprächen

Mit der Auslegung des § 100d Abs. 4 S. 1 StPO[934] geht ferner die überaus praxisrelevante Frage einher, wie zu verfahren ist, wenn die zu überwachenden Gesprächsinhalte mit hoher Wahrscheinlichkeit nur teilweise dem Kernbereich zuzuordnen sein werden (sog. Mischgespräche[935]). Die bis heute nicht abschließend geklärte Frage ringt vordergründig um das zutreffende Verständnis des § 100d Abs. 4 S. 1 StPO. Danach dürfen Maßnahmen nach § 100c StPO nur angeordnet werden, wenn tatsächliche

931 BVerfGE 109, 279, 319.
932 OLG Düsseldorf, StV 2008, 181; *Löffelmann*, ZIS 2006, 87, 91.
933 BVerfGE (abw. Meinung) 109, 279, 391.
934 Entspricht seinem Wortlaut nach dem § 100c Abs. 4 S. 1 StPO a.F.
935 Vgl. *Wolter* in: SK-StPO, § 100c StPO, Rn. 55 m.w.N.

Anhaltspunkte die Annahme rechtfertigen, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Da nach zutreffender Ansicht bereits bei zu erwartenden „beichtenden Zwiegesprächen" keine negative Kernbereichsprognose gestellt werden kann, erlangt diese Frage besondere Bedeutung, wenn die Strafverfolgungsbehörden davon ausgehen dürfen, dass es zwar zu nüchternen Deliktsbesprechung kommt, diese aber beispielsweise mit der Besprechung einer Krankheit einhergeht oder mit anderen intimen Vorgängen zu rechnen ist.

a) Weites Verständnis

Der Vorschrift ein weites Verständnis zugrunde gelegt, soll die Anordnung einer Maßnahme auch dann zulässig, wenn neben kernbereichsrelevanten Äußerungen auch mit solchen zu rechnen ist, die nicht dem Kernbereich zuzurechnen sind. Bei zu erwartenden Mischgesprächen könne daher im Ergebnis eine negative Kernbereichsprognose gestellt werden und die Maßnahme angeordnet werden.[936] Mit diesem weiten Verständnis sympathisiert auch der BGH, der aufgrund der Erwartung, dass der Beschuldigte mit seiner Ehefrau über die Tat sprechen werde und zu erwarten war, dass dieses Gespräch nicht ausschließlich privaten Charakter, sondern auch Verdunklungshandlungen zum Gegenstand habe, von einer negativen Kernbereichsprognose ausging.[937] Dass es der BGH für eine rechtmäßige Beweiserhebung als offensichtlich genügend erachtet, wenn zumindest auch Äußerungen mit entsprechendem Sozialbezug erfasst werden, wird umso deutlicher angesichts dessen, dass er trotz des Wissens, dass der Betroffene mit seiner Ehefrau auch seine außereheliche Affäre zum Tatopfer besprechen werde, kein Erhebungsverbot für notwendig erachtete.[938]

936 noch zum mit § 100d Abs. 4 S. 1 StPO inhaltsgleichen § 100c Abs. 4 S. 1 StPO a.F.: FS-Fezer/*Rogall*, S. 61, 81 ff.; *Leutheusser-Schnarrenberger*, ZRP 2005, 1, 2 f.; *Zöller*, StraFo 2008, 15, 22; bereits zu § 100d Abs. 4 S. 1 StPO: *Eschelbach* in: SSW-StPO, § 100d StPO, Rn. 15; *Großmann*, JA 2019, 241, 247; *Bruns* in: KK-StPO, § 100d StPO Rn. 6.

937 BGHSt 53, 294, Rn. 27.

938 BGHSt 53, 294, Rn. 44.

b) Enges Verständnis

Die gegenteilige Auffassung will § 100d Abs. 4 S. 1 StPO derart verstanden wissen, dass auch bei zu erwartenden Mischgesprächen eine Überwachung unterbleiben muss.[939] In diese Richtung tendierte auch das Bundesverfassungsgericht in seiner Entscheidung zum großen Lauschangriff, als es zu bedenken gab, dass es den verfassungsrechtlichen Anforderungen nicht genüge, wenn die akustischen Wohnraumüberwachung nur in dem Fall unzulässig ist, in dem sämtliche Erkenntnisse einem Verwertungsverbot unterliegen.[940] Sofern anzunehmen ist, dass auch zum Kernbereich gehörende Äußerungen aufgezeichnet werden, fehle es schlicht an den notwendigen gesetzlichen Voraussetzungen für eine negative Kernbereichsprognose.[941]

c) Stellungnahme

Aus der vor dem 24.08.2017 geltenden Rechtslage, nach der die Telekommunikationsüberwachung gem. § 100a Abs. 4 S. 1 StPO a.F. lediglich dann unzulässig war, wenn *allein* Äußerungen aus dem Kernbereich zu erwarten waren, wurde gefolgert, dass der im Vergleich hierzu strengere § 100c Abs. 4 S. 1 StPO a.F. (mangels der Einschränkung auf allein kernbereichsrelevante Gespräche) auch bereits für Mischgespräche ein Abhörgebot beinhalten müsse.[942] Seit dem 24.08.2017 normiert § 100d Abs. 1 StPO nunmehr, dass alle Maßnahmen nach § 100a StPO bis § 100c StPO (erst) dann unzulässig seien, wenn *allein* (im Sinne von ausschließlich) Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Hieraus könnte zu schließen sein, dass es dem gesetzgeberischen Willen entspricht, sodann im umgekehrten Fall eines Mischgespräches, das eben nicht ausschließlich kernbereichsrelevante Inhalte zum Gegenstand hat,

939 Insofern allesamt noch zum mit § 100d Abs. 4 S. 1 StPO inhaltsgleichen § 100c Abs. 4 S. 1 StPO a.F. *Klesczewski*, StV 2010, 458, 463; *Puschke/Singelnstein*, NJW 2008, 113, 114; FS-Böttcher/*Roxin*, S. 159, 170 f.; FS-Wolter/*Roxin*, 1057, 1068; FS-Küper/*Wolter*, S. 707, 718 f.; *Walter* in: Europäisierung des Rechts, S. 291, 295 f.; GS-Lisken/*Denninger*, 13, 19.

940 BVerfGE 109, 279, 330, zustimmend *Bergemann*, DuD 2007, 581, 584.

941 *Klesczewski*, StV 2010, 458, 463.

942 *Klesczewski*, StV 2010, 458, 463.

eine Beweiserhebung zuzulassen.[943] Andererseits normiert der für die Wohnraumüberwachung speziellere § 100d Abs. 4 S. 1 StPO, der analog zum früheren § 100c Abs. 4 StPO a.F. ausgestaltet ist, wiederum, dass eine Wohnraumüberwachung nur angeordnet werden darf, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Dies könnte wiederum derart zu interpretieren sein, dass mangels einer Beschränkung des Erhebungsverbots für den Fall ausschließlicher Kernbereichsbetroffenheit, ein solches bereits bei Mischgesprächen besteht. Die Neuregelung der Vorschriften zum Kernbereich haben daher nicht zu einer Klärung der Frage der zulässigen Überwachung von Mischgesprächen im Rahmen der Wohnraumüberwachung geführt, sondern diese Frage lediglich auf dem Papier von § 100c Abs. 4 StPO a.F. in § 100d Abs. 4 StPO verlagert. Die Aussagen des Bundesverfassungsgerichts aus dem BKAG Urteil werden jedoch in Richtung eines weiten Verständnisses des § 100d Abs. 4 StPO zu deuten sein. Hinsichtlich der mit § 100d Abs. 4 StPO im Kern inhaltsgleichen Formulierung aus § 20h Abs. 5 BKAG entschied das Gericht, dass der dadurch normierte Kernbereichsschutz auf der Erhebungsebene den verfassungsrechtlichen Notwendigkeiten genüge.[944] Dabei stelle es eine verfassungsmäßige Anwendung der Norm dar, die Vermutung für den Kernbereich als widerlegt zu erachten, wenn Gespräche zwar mit „*höchstpersönlichen Inhalten durchsetzt sind*" aber gleichwohl auch konkrete Anhaltspunkte über Straftaten enthalten.[945] In Anbetracht des hier vorgeschlagenen weiteren unabwägbaren Einzugsbereich des Kernbereichs, der auch beichtende Zwiegespräche oder Tagebucheinträge umfasst, erscheint es angemessen, solche Mischgespräche, die nüchtern berichtend, konkrete Anhaltspunkte zu Straftaten wiedergeben, auch dann überwachen zu dürfen, wenn diese Gespräche auch durch Höchstpersönliches flankiert werden. Insbesondere wäre die Wohnraumüberwachung ansonsten praktisch wertlos, da es kaum straftatenbezogene Gespräche geben wird, die ausschließlich Straftaten zum Inhalt haben.[946] Würde zwischen den Gesprächsbeteiligten ein enges Vertrauens-

943 Insofern bereits kritisch hinsichtlich der in § 100a Abs. 4 StPO a.F. enthaltenen Regelung von der Betroffenheit des Kernbereichs im Gesamten nur bei ausschließlicher Kernbereichsbetroffenheit anzunehmen, *Roggan*, StV 2011, 762, 764; *Kleih*, Die strafprozessuale Überwachung der Telekommunikation, S. 245; *Nöding,* StraFo 2007, 456, 458.

944 BverfGE 141, 220, Rn. 202.

945 BverfGE 141, 220, Rn. 198.

946 Vgl. *Zöller*, StraFo 2008, 15, 22.

verhältnis bestehen, könnte beinahe nie ausgeschlossen werden, dass auch über höchstpersönliches gesprochen wird. Die Maßnahme könnte dann nie im Bereich engster Vertrauensverhältnisse angeordnet werden, was dem Zweck der Maßnahme zuwiderliefe und eine effektive Strafverfolgung einseitig beschneiden würde.

4) Nachgelagerter Kernbereichsschutz

Eine den Kernbereich ebenfalls bereits auf Erhebungsebene schützende Funktion fällt der Unterbrechungspflicht gem. § 100d Abs. 4 S. 2 StPO zu. Wurde eine Maßnahme aufgrund einer negativen Kernbereichsprognose angeordnet, kommt es sodann aber im Rahmen der Überwachung zu Äußerungen, die dem Kernbereich angehören, ist die Überwachung zu unterbrechen. Sofern während einer Echtzeit-Überwachung eine Zuordnung zum Kernbereich nicht zweifelsfrei möglich erscheint, ist die Überwachung in Form einer automatisierten Aufzeichnung fortzuführen.[947] Durch das Fortführen der Maßnahme in Form einer automatisierten Aufzeichnung wird gleichfalls einem Hauptproblem der Echtzeit-Überwachung abgeholfen. Im Rahmen der Echtzeit-Überwachung müsste der mithörende Beamte in Sekunden entscheiden, ob eine Maßnahme dem streng geschützten Kernbereich zuzuordnen ist. Eine solche ad hoc Beurteilung wird diesen nicht selten vor erhebliche Schwierigkeiten stellen.[948] Erschwernisse stellen dabei fremde Sprachen, die Benutzung von Geheimcodes, Hintergrundrauschen oder Verbindungsproblemen dar, die das Gesprochene ohne technische Aufbereitung kaum unmittelbar verständlich verstehen lassen. Hinzu kommt, dass selbst bei klar zu vernehmenden Gesprächen die Zuordnung einer Stimme beim Mithören in Echtzeit nicht immer möglich ist, was eine Einschätzung der zwischen den Gesprächspartner bestehenden persönlichen Beziehungen erschwert.[949]

Eine fälschlicherweise vorgenommene Unterbrechung der Aufzeichnung könnte bedeuten, dass der entscheidende Tathinweis nicht aufge-

947 BverfGE 141, 220, Rn. 199, a.A.: *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 167; zurückhaltender, gar mit der Tendenz sodann gänzlich auf die Wohnraumüberwachung zu verzichten noch BverfGE 109, 279, 324; BVerfG, NJW 2007, 2753, 2757.

948 *Büddefeld*, Kriminalistik 2015, 204, 206; *Brocker/Zartmann*, DriZ 2005, 108, 109, *Kötter*, DÖV 2005, 225, 230.

949 BverfGE 129, 208, 248; BverfGE 120, 274, 338; *Käß*, BayVBl 2008, 225, 232; *Haas*, NJW 2004, 3082, 3083.

zeichnet wird. Würde eine Live-Überwachung wiederum fälschlicherweise fortgesetzt, obwohl kernbereichsspezifische Inhalte thematisiert werden, würde es zu einer Kenntnisnahme dieser Informationen unmittelbar durch die Ermittlungsbeamten kommen. Unter diesen Aspekten erscheint mittels der automatisierten Aufzeichnung sowohl dem Interesse der Strafverfolgung, einer möglichst umfassenden Aufzeichnung sämtlicher verwertbarer Informationen als auch dem Interesse des Beschuldigten, eine Kenntnisnahme kernbereichszugehöriger Informationen durch die Ermittlungsbeamten zu verhindern, gedient. Bei der automatisierten Überwachung, die sämtliche Gespräche im gewünschten Zeitraum ununterbrochen aufzeichnet, kommt es schließlich erst auf Ebene der Verwertbarkeit zur Kontrolle und zur Löschung kernbereichsspezifischer Informationen. Eine staatliche Kenntnisnahme der aufgezeichneten Informationen ist dann unumgänglich, wird allerdings wenigstens nicht – wie im Falle der Echtzeit-Überwachung – durch den eingesetzten Ermittlungsbeamten, sondern durch eine externe Kontrollbehörde vorgenommen. Ist ein effektiver Kernbereichsschutz damit einmal nicht bereits auf Erhebungsebene gewährleistet, muss durch einen nachgelagerten Kernbereichsschutz sichergestellt werden, dass mögliche kernbereichsrelevante Informationen vor der Kenntnisnahme der aufgezeichneten Informationen durch die Strafverfolgungsbehörden herausgefiltert werden.[950]

a) Umfang nachgelagerter Kontrollen

Im Detail unterscheidet sich der Umfang nachgelagerter Kontrollen je nach angeordneter Überwachungsmethode, der Art deren Durchführung und der damit typischerweise einhergehenden Gefahr kernbereichsrelevante Inhalte aufzugreifen.[951] Hinsichtlich der Durchführungsart kann jede heimliche Überwachungsmethode im Wege einer Echtzeit-Überwachung oder als automatisierte Überwachung erfolgen. Die Echtzeit-Überwachung stellt dabei die flexiblere Überwachungsmethode dar, da sie die Möglichkeit beinhaltet, die Aufzeichnung zu unterbrechen, wenn während der Überwachung kernbereichsrelevante Informationen hervortreten. Daher wird sie gerade dann zum Einsatz kommen, wenn die Eigenart der Überwachung die Erhebung kernbereichsspezifischer Daten kaum ausschließen kann und daher ein menschliches Eingreifen öfters von Nö-

950 BverfGE 141, 220, Rn. 128 f., 220 ff.
951 BverfGE 141, 220, Rn. 129.

ten sein wird.[952] Dies macht die Echtzeit-Überwachung zur grundsätzlich eingriffsmilderen Maßnahme, da eindeutig kernbereichsrelevante Inhalte von vornherein nicht aufgezeichnet werden.[953] Ferner beeinflussen die Charakteristika der angeordneten Maßnahme die Notwendigkeit einer nachgeordneten Verwertbarkeitskontrolle. Wenn beispielsweise eine Maßnahme wie die Telekommunikationsüberwachung vorliegt, die in ihrem Gesamtcharakter nicht in gleicher Weise wie die Wohnraumüberwachung oder auch die Online-Durchsuchung durch ein Eindringen in die Privatsphäre geprägt ist, wird sich eine Sichtung durch eine unabhängige Stelle auf Zweifelsfälle beschränken können.[954] Bei der Wohnraumüberwachung hingegen muss eine vollständige Vorlage der erlangten Informationen – gleich ob diesen eine automatisierte Überwachung oder eine solche in Echtzeit zugrunde lag – an eine externe Stelle erfolgen.[955] Eine Beschränkung auf Zweifelsfälle genügt aufgrund der größeren Kernbereichsnähe einer Wohnraumüberwachung nicht.[956]

Die generelle Verwertbarkeitskontrolle solcher Informationen, die durch eine Wohnraumüberwachung gewonnen wurden, wird als zu eng und Verkomplizierung der Effektivität dieser Maßnahme, kritisiert.[957] Diese Kritik muss allerdings im Lichte der dem Urteil zugrunde liegenden Thematik betrachtet werden. Angesichts der Aufgabe des BKAG in Form der Gefahrenabwehr wird oftmals eine unverzügliche Reaktion auf neue Erkenntnisse erforderlich sein, wobei diesem Ziel ein weiterer Prüfungsschritt tatsächlich in gewisser Weise entgegenstehen könnte.[958] Bei der Verfolgung repressiver Zwecke anhand der StPO kann die durch einen weiteren Kontrollschritt entstehende Verkomplizierung durch die damit einhergehende möglichst umfassende Wahrung der Grundrechte des Betroffenen, dagegen legitimiert werden. Schließlich ist der Strafverfolgung – im Unterschied zur Gefahrenabwehr – ein dringliches und sofortiges Handeln gerade nicht immanent.

---

952 BT-Drs. 15/4533, S. 15; BverfGE 109, 279, 324.
953 *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 167.
954 BverfGE 141, 220, Rn. 238, 241.
955 BverfGE 141, 220, Rn. 204.
956 BverfGE 109, 279, 334; BVerfG, BverfGE 141, 220, Rn. 244 f.
957 BverfGE 141, 220, 370 f. (abw. Meinung *Schluckebier*).
958 BverfGE 141, 220, 370 (abw. Meinung *Schluckebier*); die Herausfilterung kernbereichsrelevanter Informationen durch eine unabhängige Behörde als „lebensfremd" und in jedem Falle als erhebliche Verzögerung der Vorgänge bezeichnend, *Wiemers*, NVwZ 2016, 839, 841.

b) Zusammenspiel der praktischen Möglichkeiten zum Schutz des Kernbereichs

Insgesamt besteht zwischen der Verpflichtung zur nachgelagerten Kontrolle und der Kontrolle bereits auf Erhebungsebene eine Art Wechselwirkung. Wird zum einen die Prognose hinsichtlich der Kernbereichsbetroffenheit auf der Erhebungsstufe bereits sehr eng verstanden, werden Zweifelsfälle weitgehend ausgeschlossen sein. Generell gilt, dass eine Prüfung durch eine unabhängige Stelle umso eher unterbleiben kann, je zuverlässiger bereits im Rahmen der Beweiserhebung die Erfassung kernbereichsrelevanter Sachverhalte vermieden wird.[959] Ist ein verlässlicher Stopp der Überwachung auf Erhebungsebene dabei aufgrund einer automatisierten Überwachung nicht möglich, könne und müsse der verfassungsrechtliche garantierte Kernbereichsschutz auf die Auswertungsebene verlagert werden.[960] Aus der Entscheidung des Bundesverfassungsgericht zum BKAG wird dabei teilweise gefolgert, dass die Rechtsprechung dazu über gehen könnte, dem Kernbereichsschutz zukünftig allgemein vermehrt durch nachgelagerte Verwertbarkeitskontrollen Rechnung zu tragen und Eingriffe auf der Erhebungsebene zunächst zu tolerieren.[961] Ob sich dies tatsächlich bewahrheiten wird bleibt abzuwarten, schließlich gab das Gericht im selben Urteil ebenso zu bedenken, dass der Staat selbst bei überragenden Interessen der Allgemeinheit nicht in den aus Art. 1 Abs. 1 GG abgeleiteten absolut geschützten Bereich privater Lebensgestaltung eingreifen dürfe.[962] Zu einer Beeinträchtigung des Kernbereichs würde es bei einer automatisiert ablaufenden Überwachung mangels Stoppmöglichkeiten allerdings unweigerlich kommen. Aus dem Umstand, dass beim Zugriff auf informationstechnische Systeme, beispielsweise im Rahmen einer Online-Durchsuchung, die automatisierte Überwachung als gängige Methode anerkannt ist,[963] darf ferner nicht geschlossen werden, dass das Gericht diese Vorgehensweise zukünftig auch für die Wohnraumüberwachung als gangbaren Weg erachten wird. Dass das Bundesverfassungsgericht im Rahmen der Online-Durchsuchung den Kernbereichsschutz auf Erhebungsebene etwas zurücknimmt, ist vielmehr dem spezifischen Charakter des

959 BverfGE 141, 220, Rn. 129, 241.
960 *Hoffmann-Riem*, JZ 2008, 1009, 1021; *Dammann*, Der Kernbereich der privaten Lebensgestaltung, S. 42.
961 *Dürr*, JA 2019, 432, 436.
962 BverfGE 141, 220, Rn. 120.
963 BverfGE 120, 274, 337; BverfGE 141, 220, Rn. 218.

Zugriffs auf informationstechnische Systeme geschuldet. Zum einen zielt der Kernbereichsschutz bei der Online-Durchsuchung im Unterschied zur Wohnraumüberwachung nicht vordergründig auf die Verhinderung des Aufzeichnens eines nur flüchtigen, höchstvertraulichen Moments ab, sondern soll verhindern, dass höchstvertrauliche Informationen aus einem ohnehin nur digital vorliegenden Datenbestand herausgelesen werden.[964] Zum anderen bringt der erforderliche Zugriff mittels eines Ausforschungsprogramms mit sich, dass auf Erhebungsebene lediglich ein vollständiger Datenzugriff oder überhaupt kein Datenzugriff möglich ist.[965] Dadurch wird offensichtlich, dass die schnell fortschreitende technologische Entwicklung und bestimmte daran anknüpfende automatisierte und vorprogrammierte Ermittlungseingriffe den neu gefassten § 100d StPO zunehmend leerlaufen lassen. Diesem Umstand könnte nur dadurch abgeholfen werden, wenn es möglich wäre, auch bei automatisierten Überwachungen zu verhindern, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen werden. Doch ist es technisch nach heutigen Stand kaum umsetzbar, die Spähsoftware derart einzuschränken, dass solche Daten nicht erhoben werden.[966] Zwar gilt der Schutz des Kernbereichs formal selbstredend gerade dann, wenn mit wachsenden Überwachungsmöglichkeiten, der Kernbereich bei Ermittlungen auf informationstechnische Systeme zunehmend gefährdet wird.[967] Praktisch zeichnet sich hierbei aufgrund der eingeschränkten technischen Möglichkeiten jedoch ein anderes Bild, sodass regelmäßig lediglich die nachträgliche Kernbereichskontrolle und damit die nachträgliche Möglichkeit bleibt, festzulegen was noch und was nicht zum Kernbereich gehört. Hinzu kommt, dass, selbst bei einer unterstellten technischen Einschränkbarkeit der Spähsoftware, weder die Kriterien normiert wurden, anhand derer eine Einschränkung der Spähsoftware vorgenommen werden könnte, noch – wie bereits gesehen – der Versuch unternommen wurde, die vagen Definitionsansätze des Kernbereichs weiter zu konkretisieren.[968]

964 BverfGE 141, 220, Rn. 218.
965 BverfGE 141, 220, Rn. 218; vgl. auch *Gless*, StV 2018, 671, 676.
966 *Gless*, StV 2018, 71, 675.
967 BverfGE 120, 378, 429.
968 *Gless*, StV 2018, 71, 675; vgl. § 5, A), I), 1), c).

c) Stellungnahme

Generell bleibt die dem nachgelagerten Kernbereichsschutz zugrunde liegende automatisierte Überwachung daher kritisch zu betrachten und muss auf das absolut notwendige Minimum begrenzt bleiben. Schließlich muss bei einer erstmal erfolgten staatlichen Kenntnisnahme kernbereichsrelevanter Informationen – sei es auch durch eine externe Behörde – stets die Gefahr eines Missbrauchs dieser Informationen, im Gefühl effektiver Strafverfolgung einen Straftäter seiner Strafe zuzuführen, bedacht werden. Hinzu kommt, dass der Mensch solche Informationen, die er einmal gehört oder gelesen hat, nicht einfach aus seinem Gedächtnis streichen kann. Gerade wenn (erhebliche) Straftaten im Raum stehen, wäre es letztlich wohl gar verständlich, wenngleich rechtswidrig, wenn diese Informationen unterbewusst Eingang in das Handeln der entsprechenden Personen finden würden.[969]

Priorisiert werden sollte daher stets, sofern (technisch) umsetzbar, die Durchführung einer Live-Überwachung, mit der Möglichkeit der Unterbrechung, sodass entsprechende Informationen von vornherein nicht vernommen werden. Anzuregen ist in solchen Fällen ebenso eine nachgeordnete Durchsicht der Daten dahingehend vorzunehmen, ob die Behörden im Rahmen der Live-Überwachung sorgfältig gearbeitet haben und der Kernbereichsschutz umfassend gewährleistet wurde.[970] Vor dem Hintergrund der grundrechtsintensiven Wohnraumüberwachung kann dies nicht an Kapazitätsgründen scheitern, zumal es Aufgabe des Staates ist, ein die Grundrechte des Betroffenen wahrendes Ermittlungsverfahren zu garantieren.[971] Vor dem Hintergrund der vergleichsweise geringen Anzahl an angeordneten Wohnraumüberwachung erscheint die daraus resultierende Mehrbelastung auch vertretbar.[972] Angesichts der Prognoseunsicherheiten, unter denen Strafverfolgungsbehörden arbeiten, kann zwar nicht jedes unbeabsichtigte Eindringen in den Kernbereich auf Erhebungsebene ausgeschlossen und daher auch nicht jede tatsächliche Erfassung von höchstpersönlichen Informationen einen Verfassungsverstoß begründen.[973] Den-

969 Vgl. m.w.N. *Löffelmann*, JR 2009, 10, Fn. 3; *Geipel*, Handbuch der Beweiswürdigung, § 25, Rn. 55.

970 So auch *Dürr*, JA 2019, 432, 437.

971 Vgl. *Roggan*, StV 2011, 762, 764 wonach letztlich bloße fiskalische Belange über kein überragendes verfassungsrechtliches Gewicht verfügen.

972 *Büddefeld*, Kriminalistik 2015, 204, 206.

973 BverfGE 141, 220, 278, vgl. dazu auch *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 245, der vorschlägt angesichts

noch würde es den durch das Bundesverfassungsgericht aufgestellten Maßstäben zum Schutz Kernbereiches nicht genügen, einen staatlichen Eingriff in den Kernbereich auf Erhebungsebene, unabhängig bestehender Möglichkeiten dieses Risiko zu minimieren, zunächst stets hinzunehmen und sodann erst auf Verwertungsebene durch die Datenlöschung final zu „korrigieren".

5) Der Kernbereichsschutz bei übrigen Maßnahmen

Naturgemäß kommt dem Kernbereichsschutz bei der Wohnraumüberwachung als grundrechtsintensivster Überwachungsmethode die größte Relevanz zu. Dies macht einen entsprechenden Kernbereichsschutz bei anderen Ermittlungsmaßnahmen allerdings nicht entbehrlich. Bereits § 100d Abs. 1 StPO erklärt neben § 100c StPO auch Maßnahmen nach § 100a und § 100b StPO bei einer zu erwartenden Betroffenheit des Kernbereichs für unzulässig. Im Unterschied zur Wohnraumüberwachung wird der Kernbereichsschutz wie bereits angedeutet bei der Online-Durchsuchung, sofern keine Live-Online-Überwachung stattfindet, primär auf Verwertungsebene verwirklicht.[974] Dies liegt darin begründet, dass bei der Durchführung einer Online-Durchsuchung in der Regel kaum vorhersehbar ist, welchen Inhalt die erhobenen Daten haben werden.[975] Eine Kernbereichsprognose anhand der Indikatoren, die das Bundesverfassungsgericht im Rahmen der Wohnraumüberwachung aufgestellt hat, ist lediglich auf den Fall einer Live-Online-Überwachung übertragbar; nicht jedoch auf die offline Durchsuchung der sich auf der Festplatte des Computers befindlichen Daten. Diese werden daher automatisiert erhoben und anschließend auf Verwertungsebene auf eine Kernbereichsbetroffenheit untersucht.

Durch den Gesetzgeber geklärt wurde die bis in das Jahr 2019 offene Frage eines Kernbereichsschutz im Rahmen des § 100f StPO. Seit dem 26.11.2019 verweist § 100f Abs. 4 StPO auf die kernbereichsschützenden

---

dieses auch im Rahmen einer Live-Überwachung teilweise unvermeidlichen Umstandes, nicht mehr von einem „absolut geschützten Kernbereich privater Lebensführung", sondern stattdessen von der „absolut geschützten Achtung des Kernbereichs der privater Lebensgestaltung" zu sprechen.

974 BverfGE 120, 274, 337 f.; Schmidt-Bleibtreu/*Hofmann*, Art. 2 GG, Rn. 39.

975 BverfGE 120, 274, 337 f.

Vorschriften des 100d Abs. 1 und 2 StPO.[976] Vorausgegangen war dem die Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz, in welcher das Gericht für den § 20g BKAG – das Pendant zum repressiven § 100f StPO – explizit forderte, dass zur Verfassungsmäßigkeit einer solchen Vorschrift, diese auch Regelungen zum Kernbereichsschutz enthalten müsse.[977] Auch außerhalb von Wohnungen sind Überwachungsmaßnahmen möglich, die typischerweise tief in die Privatsphäre eindringen.[978]

Während der Kernbereichsschutz für die verdeckten Ermittlungsmaßnahmen der §§ 100a, 100b, 100c sowie § 100f StPO gesetzlich kodifiziert ist und mit Ausnahme der automatisiert ablaufenden Online-Durchsuchung bereits auf Erhebungsebene zum Tragen kommt, stellt sich die Frage, wie der Kernbereichsschutz bei den offenen Ermittlungsbefugnissen verwirklicht wird. Obwohl auch durch offene Ermittlungsmaßnahmen entdeckte Beweismittel eine Kernbereichsrelevanz aufweisen können, finden sich für die Durchsuchung oder die Beschlagnahme keine entsprechenden Regelungen.[979] Dies bedeutet gleichfalls nicht, dass der Kernbereichsschutz bei solchen Maßnahmen keine Bedeutung zukommt. Da offene Maßnahmen in der Regel mit einem weniger intensiven Eingriff in die Grundrechte des Betroffenen einhergehen und in der Regel keine Kernbereichsrelevanz aufweisen, genügt es den Kernbereichsschutz auf Verwertbarkeitsebene – beispielsweise im Falle eines beschlagnahmten Tagebuchs – zu berücksichtigen.

6) Übertragung der Maßstäbe auf die Nutzung eines Smart Speaker zur Strafverfolgung

Zu klären ist, wie die über das Endgerät des Sprachassistenten generierte Informationen im Hinblick auf eine etwaige Kernbereichsrelevanz bzw.

976 Im Zuge des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679.

977 BverfGE 141, 220, Rn. 175; bereits vor dieser Entscheidung dies fordernd *Bergemann*, DuD 2007, 581, 583, *Reiß,* StV 2008, 539, 542; *Paa*, Der Zugriff der Strafverfolgungsbehörden auf das Private, S. 188, *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, S. 382.

978 BverfGE 141, 220, Rn. 176; *Paa*, Der Zugriff der Strafverfolgungsbehörden auf das Private, S. 188.

979 *Kretschmer*, HRRS 2010, 551, 557; *Zöller*, StraFo 2008, 15, 22; *Warg*, NStZ 2012, 237, 238 f.

im Vorfeld der Maßnahme zu stellende negative Kernbereichsprognose einzuordnen sind.

a) Überwachung mündlicher Informationsabfragen während aktiver Nutzung des Smart Speaker

Zu denken ist dabei an den Fall, in dem eine aktive und bewusste Informationsabfrage an den Sprachassistenten § 100b StPO im Rahmen einer Live-Online-Überwachung oder im Zuge einer Maßnahme nach § 100c StPO aufgezeichnet wird. Handelt es sich bei der Informationsabfrage um eine Art Selbstgespräch, sodass die Erhebung und anschließende Verwertbarkeit gänzlich ausgeschlossen wäre oder sind die Maßstäbe, die auf Zwiegespräche und Tagebucheinträge Anwendung finden auch hier in Ansatz zu bringen, sodass die Erhebung einer Informationsabfrage nicht generell unterbleiben muss bzw. zu stoppen ist.

Das Surfen im Internet – das letztlich auch der Nutzung eines Sprachassistenten zugrunde liegt – und dessen Überwachung durch die Strafverfolgungsbehörden war erstmals Gegenstand der höchstrichterlichen im Rahmen einer BGH-Entscheidung, die sich mit Überwachung eines Terrorverdächtigen aus dem möglichen Umfeld von Al-Quaida beschäftigte.[980] Der Beschluss lässt jedoch eine tiefergehende Auseinandersetzung mit der verfassungsrechtlichen und strafprozessualen Bewertung des Surfverhaltens vermissen.[981] Der zweite Senat des Bundesverfassungsgerichts äußerte sich schließlich in der „Surfen im Internet" Entscheidung[982] im Jahr 2016 zu der Frage, inwieweit der Kernbereichsschutz einer Überwachung des Surfverhaltens im Internet nach § 100a StPO entgegenstehen könnte. Dabei gab es zwar zu, dass sich bei der Überwachung aufgerufener HTML-Seiten „ein quantitatives Mehr" an überwachter Kommunikation als bei der Telefonüberwachung ergebe.[983] Dieser Masse stehe dennoch der lediglich *„fragmentarische Inhalt"* der einzelnen Informationsrecherche gegenüber.[984] Dabei geht das Bundesverfassungsgericht davon aus, dass die Strafverfol-

980 *BGH*, NStZ-RR 2011, 148.
981 *Albrecht/Braun*, HRRS 2013, 500, 502.
982 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 = teilweise in NJW 2016, 3508 ff.
983 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 47 = teilweise in NJW 2016, 3508 ff.
984 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 47 = teilweise in NJW 2016, 3508 ff.

gungsbehörden bei einer Überwachung des Surfverhaltens lediglich sehr kurze Einzelakte zur Kenntnis nehmen können, da gerade beim Surfen im Internet lediglich eine oberflächliche Kommunikation stattfinde.[985] Ohnehin betreffe der Aufruf einer einzelnen Web-Seite häufig überhaupt nicht den Kernbereich der Persönlichkeit.[986] Das Gericht kommt daher zu dem Schluss, dass Akte der höchstvertraulichen Lebensführung letztlich nur einen kleinen Teil des Surfverhaltens darstellen. Selbst wenn dieser kleine Teil bei der Überwachung erfasst werden könnte, sei er nicht – wie die Überwachung des Rückzugsbereichs der Wohnung – „typusprägend" für die Persönlichkeit des Betroffenen.[987] Diese im Kontext des § 100a StPO getroffene Entscheidung verdeutlicht, dass das Gericht beim bloßen Surfen und der damit verbundenen Informationsabfrage keine Veranlassung sah, diesem Verhalten den besonderen Kernbereichsschutz zuzusprechen.[988] Wenngleich sich die einschlägige Ermächtigungsgrundlage für eine Überwachung eines Sprachassistenten vom in der zitierten Entscheidung maßgeblichen § 100a StPO unterscheidet, so handelt es sich bei dem Zugriff auf eine konkrete Informationsabfrage, dennoch um eine mit der Überwachung des Surfverhaltens nach § 100a StPO inhaltlich vergleichbaren Sachverhalt. Für den Inhalt und damit die strafprozessuale Bedeutung der getätigten Informationsabfrage macht es keinen Unterschied, ob diese analog über eine Computertastatur oder auditiv über einen Sprachassistenten erfolgt.

Der erste Senat des BVerfG stellt dagegen in der Entscheidung zum BKA-Gesetz klar, dass die Telekommunikationsüberwachung gemessen an ihrem Gesamtcharakter nicht in gleicher Weise in die Privatsphäre eindringt, wie dies bei der Wohnraumüberwachung oder auch der Online-Durchsuchung der Fall ist.[989] Typischerweise sei der Teil der höchstpersönlichen Kommunikation lediglich ein kleiner Teil des Verhaltens, das bei der Telekommunikationsüberwachung miterfasst zu werden droht.[990] Allerdings ließ sich das Gericht dabei von der Grundvorstellung leiten, dass sich die Telekommunikationsüberwachung in der Regel auf einzelne

985 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 47 = teilweise in NJW 2016, 3508 ff.
986 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 47 = teilweise in NJW 2016, 3508 ff.
987 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 47 = teilweise in NJW 2016, 3508 ff.
988 Zustimmend *Bär*, ZD 2017, 132, 137.
989 BverfGE 141, 220, Rn. 238.
990 BverfGE 141, 220, Rn. 238.

Akte unmittelbarer Kommunikation bezieht und nicht wie beispielsweise eine Online-Durchsuchung, das Nach- oder Mitverfolgen der Aktivitäten im Internet über einen längeren Zeitraum ermöglicht und so auf geheime Schwächen oder Neigungen schließen lässt.[991] Durch die Überwachung der Nutzung eines Sprachassistenten wird jedoch gerade das Nachverfolgen der Bewegungen im Internet ermöglicht. Den Maßstab des ersten Senats zugrunde gelegt, könnte daher zu schlussfolgern sein, dass die Eingriffsintensität des Nachverfolgens des Surfverhaltens der einer Online-Durchsuchung durchaus gleichkommt. Die Online-Durchsuchung wiederum ist ihrem Gesamtcharakter nach aber durch ein erhebliches Eindringen in die Privatsphäre geprägt. Daher könnte anzunehmen sein, dass der erste Senat im Unterschied zum zweiten Senat bei der Überwachung des Surfens im Internet, insbesondere aufgrund der Möglichkeit infolge einer systematischen Auswertung des Surfverhaltens und der daran anknüpfenden Möglichkeit im Rahmen einer Gesamtschau ein Persönlichkeitsprofil zu erstellen, diesem Vorgang die Kernbereichsrelevanz nicht abgesprochen hätte.

Der Karlsruher Einschätzung im Rahmen der „Surfen im Internet" Entscheidung ist jedenfalls zu entgegen, dass diese in ihrer Pauschalität der Sensibilität der Internetnutzung vieler Menschen nicht gerecht wird.[992] Die Bandbreite und Intensität der Internetnutzung umfasst heute Themengebiete aller Lebensbereiche. Von persönlichen Neigungen über Fragen der Gesundheit bis hin zur bloßen Unterhaltung dient die Nutzung des Internet all diesen Bedürfnissen. Aufgrund der scheinbaren Anonymität und Abgeschiedenheit wird der Betroffene über das Internet Antworten auf Bedürfnisse suchen, denen nachzugehen er sich ansonsten scheut. Im Unterschied zu einem Zwiegespräch vor Ort, via Telefon, E-Mail oder per Chat, gibt der Betroffene bei der Nutzung eines Sprachassistenten gerade nicht bewusst und freiwillig Wissen gegenüber einem Dritten preis. Er ist damit nicht bereit, sich des Schutzes der Privatsphäre zu ergeben. Hinzu kommt, dass der sich des Internets bedienende Nutzer keineswegs seine Daten dem Zugriff anderer preisgeben will. Im Gegenteil versucht sich der Nutzer vor „Hacker"-Angriffen durch die Installation diverser Firewalls zu schützen.[993] Mit der Nutzung des Internets wird daher stets ein persönlicher Geheimhaltungswille einhergehen. Aus diesen Umständen wird teilweise gefolgert, dass die fehlende Interaktion mit Dritten die Informa-

991 BverfGE 141, 220, Rn. 238.
992 *Hiéramente*, HRRS 2016, 448, 451.
993 *Kutscha*, NJW 2007, 1169, 1170.

tionsabfrage gar näher in Verbindung zu einem Selbstgespräch oder Tagebucheintrag als einem Zwiegespräch bringe.[994] In jedem Fall erscheint es die Realität der Internetnutzung nicht sachgerecht widerzuspiegeln, wenn die hierdurch hinterlassenen Spuren unproblematisch keine Kernbereichsrelevanz aufweisen sollen. Gleichsam muss beachtet werden, dass einer strikten Übernahme der zu den Selbstgesprächen ergangenen Rechtsprechung entgegensteht, dass sich bereits der durchschnittliche Internetnutzer darüber im Klaren sein muss, dass er bei dessen Nutzung Spuren hinterlässt. Sowie bereits bei der Vornahme eines klassischen Telefongesprächs bedacht werden musste, dass womöglich Dritte mithören,[995] so steigt auch bei der Nutzung eines Sprachassistenten über das Internet das Bewusstsein der Bevölkerung, dass möglicherweise Dritte ihre Aussagen mithören könnten. Hinzu kommt, dass die Speicherung der Audiodateien in der Cloud des Dienstleistungsanbieters zu einer Manifestation dieser Daten führt, die so lange bestehen bleibt, bis sich der Betroffene zur Löschung seiner Aufzeichnungen aus der Cloud entscheidet. In der Konsequenz kann eine Informationsabfrage daher kaum die gleiche Stufe der Schutzwürdigkeit wie ein tatsächliches Selbstgespräch erreichen.[996] In Kenntnis des Hinterlassens von Spuren und der damit einhergehenden Manifestation der vollzogenen Abfragen kann eine mündliche Informationsabfrage nicht mit der Vornahme eines Selbstgesprächs verglichen werden. Zwar wird der Betroffene die Handlung in der Annahme der Vertraulichkeit vornehmen, wohingegen ihm aber gleichwohl bewusst sein muss, dass seine Informationsabfragen konserviert werden. Die vielzitierte Flüchtigkeit des gesprochenen Wortes kommt einer solchen Informationsabfrage daher gerade nicht zu. Es handelt sich bei der Informationsabfrage über einen Sprachassistenten daher nicht generell um ein ohne Rücksicht auf die Gegebenheiten des Einzelfalls der Beweiserhebung grundlegend entzogenes Selbstgespräch. Im Unterschied zum Verfassen eines Tagebuches wiederum wird es sich im Falle der Informationsbeschaffung oder Befehlsausführung mittels des Sprachassistenten in der Regel nicht um ein „Diktat des Gewissens“[997] handeln. Vielmehr wird der Nutzer den Sprachassistenten auffordern, ihm Informationen zu bestimmten Themengebieten zu übermitteln. Auch wenn diese Aufforderung ihren Ursprung im Inneren

994 *Hiéramente*, HRRS 2016, 448, 451.
995 *Hirsch* in: Zwiehoff, Der große Lauschangriff, XII.
996 *Hiéramente,* StraFo 2013, 96, 101.
997 *Amelung*, NJW 1990, 1753, 1759.

der Persönlichkeit haben kann,[998] werden einzelne Informationsabfragen selten einen solch umfassenden Einblick in die Persönlichkeit gewähren, wie dies ein kompletter Tagebucheintrag, der Gefühle und Empfindungen des Verfassers zum Ausdruck bringt, ermöglicht. Kommt es folglich im Rahmen einer Echtzeitüberwachung zur Nutzung eines Sprachassistenten, wird diese regelmäßig nicht aufgrund einer zu erwartenden Kernbereichsbetroffenheit unterbrochen werden müssen.

b) Einsatz eines Sprachassistenten als Wanze

Sofern der Sprachassistent als Wanze im Sinne des § 100c StPO eingesetzt wird und unabhängig von einer aktiven Nutzung des Sprachassistenten eine Überwachung stattfindet, ergibt sich keine neue Situation im Vergleich zur klassischen Wohnraumüberwachung. Während das Abhören eines Selbstgespräches über den Sprachassistenten in sämtlichen Fällen unterbleiben muss, gilt für ein über dieses Medium überwachtes Zwiegespräch, dass ein hierbei erwarteter Straftatenbezug noch nicht per se die Annahme einer negativen Kernbereichsprognose rechtfertigt. Entscheidend ist die Frage, inwiefern das ablaufende Gespräch durch die Äußerung von Gefühlen, Empfindungen, und Ansichten eine Art der Selbstreflexion darstellt, die für das ablaufende Gespräch prägend ist. Sofern dies der Fall ist, kann der Straftatenbezug dem erwarteten Zwiegespräch den Kernbereichsschutz nicht entziehen.

II) Beweismittelverbote und Beweismethodenverbote

Die Relevanz der Beweismittelverbote sowie der Beweismethodenverbote im Zusammenspiel mit dem Zugriff auf Sprachassistenten ist gering. Selbstredend sind auch in diesem Zusammenhang die untersagten Methoden der Beweisgewinnung wie sie insbesondere in § 136a Abs. 1, 2 StPO aufgezählt sind, zu beachten.

998 Vgl. *Hiéramente,* StraFo 2013, 96, 101 „man ist was man googelt".

B. Beweisverwertungsverbote

Bei der Beurteilung eines Beweisverwertungsverbots ist zunächst zwischen selbstständigen und unselbstständigen Beweisverwertungsverboten zu unterscheiden.[999] Steht bereits ein Verstoß im Rahmen der Beweiserhebung im Raum und ist die Frage, ob sich hieraus ein Beweisverwertungsverbot entwickelt, so ist von einem unselbstständigen Beweisverwertungsverbot die Rede.[1000] Unselbstständige Beweisverwertungsverbote bestehen in Form geschriebener und ungeschriebener Beweisverwertungsverbote.[1001] Mit Blick auf die geschriebenen Beweisverwertungsverbote ist beispielsweise § 136a Abs. 3 S. 2 StPO zu nennen, der ein Verstoß gegen ein Beweiserhebungsverbot in Form eines Beweismethodenverbots mit einem unselbstständigen geschriebenen Beweisverwertungsverbot belegt. Ferner § 100d Abs. 2 S. 2 StPO für Fälle eines Beweisthemaverbotes betreffend den streng geschützten Kernbereich oder § 257c Abs. 4 S. 3 StPO hinsichtlich des Geständnisses des Angeklagten beim Entfall der Bindungswirkung einer erfolgten Verständigung. Da es für den Gesetzgeber nicht möglich war, sämtliche mögliche Konstellationen gesetzlich zu verankern, werden die unselbstständigen geschriebenen Beweisverwertungsverbote durch unselbstständige ungeschriebene Beweisverwertungsverbote ergänzt. Ob ein solches Beweisverwertungsverbot vorliegt, folgt sodann nicht mehr aus einer an die rechtswidrige Beweiserhebung anknüpfenden Vorschrift. Vielmehr ist die Entstehung eines Beweisverwertungsverbotes in einem solchen Fall seit Jahren unter Heranziehung verschiedenster Begründungsansätze streitig.[1002]

Bei einem selbstständigen Beweisverwertungsverbot war die Beweiserhebung als solche hingegen rechtmäßig. Ein selbstständiges Beweiserhebungsverbot kann sich daher nicht aus den Verfahrensvorschriften der StPO ergeben (der Akt der Beweiserhebung ist schließlich nicht zu beanstanden), jedoch aus anderen übergeordneten Gründen, die beispielsweise der Verfassung entstammen können.[1003]

---

999 *Rogall*, ZStW 1979, 1, 3 f.; *Jahn*, JuS 2012, 85, 86.
1000 *Beulke/Swoboda*, Strafprozessrecht, Rn. 704.
1001 *Finger*, JA 2006, 529, 530.
1002 Vgl. *Schmitt* in: Meyer-Goßner/Schmitt, Einl., Rn. 55 ff.
1003 *Kudlich* in: MüKo-StPO, Einl., Rn. 450; *Paul*, NStZ 2013, 489, 490; *Beulke/Swoboda*, Strafprozessrecht, Rn. 704; *Finger,* JA 2006, 529, 530.

I) Unselbstständige Beweisverwertungsverbote

Erfolgt daher die Beweiserhebung, obwohl diese hätte unterbleiben müssen, so ist zu klären, wie mit den nun einmal vorhandenen, den Täter möglicherweise belastenden, Informationen umgegangen werden muss.

1) Geschriebene Beweisverwertungsverbote

Bei unselbstständigen geschriebenen Beweisverwertungsverboten muss stets zwischen absoluten und relativen Beweisverwertungsverboten unterschieden werden. Bei absoluten Beweisverwertungsverboten besteht für eine Gewichtung hinsichtlich Für und Wider einer Verwertung kein Raum.[1004] Die Unverwertbarkeit wird durch den Gesetzgeber final festgelegt. Bei relativen Beweisverwertungsverboten wird durch den Gesetzgeber nicht das Ergebnis, sondern lediglich die hierbei zu gewichtenden Kriterien bestimmt.[1005] So unterliegen beispielsweise den Kernbereich betreffende Informationen einem unselbstständigen geschriebenen absoluten Beweisverwertungsverbot nach § 100d Abs. 2 StPO. Das gleiche gilt nach § 100d Abs. 5 S. 1 StPO für Informationen, die durch Maßnahmen nach § 100b oder § 100c StPO aus einem Vertrauensverhältnis zu einer nach § 53 StPO geschützten Berufsgruppe entstammen. Im Unterschied hierzu sieht dagegen beispielsweise § 100d Abs. 5 S. 2 StPO für Informationen, die aus dem Verhältnis zu einer nach § 52 und § 53a StPO zeugnisverweigerungsberechtigten Person herrühren, nur ein relatives Beweisverwertungsverbot vor. Den gesetzgeberischen Vorstellungen nach besteht im Unterschied zu einem Gespräch mit einem Berufgeheimnisträger kein absoluter Vorrang des Geheimhaltungsinteresses im Hinblick auf die in §§ 52, 53a StPO genannten Personen, sodass auch die in einem solchem Verhältnis offenbarten Informationen verwertet werden dürfen, wenn die Verwertbarkeit unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zum Strafverfolgungsinteresse steht, § 100d Abs. 5 S. 2 StPO.

1004 Vgl. insofern § 160a Abs. 1 S. 2 StPO; sowie die im Zusammenhang dieser Arbeit weniger relevanten §§ 136a Abs. 3 S. 2, 81a Abs. 3, 81c Abs. 3 S. 5, 108 Abs. 2 StPO, sowie außerhalb der StPO § 393 Abs. 2 AO oder § 97 Abs. 1 S. 3 InsO.

1005 Vgl. hinsichtlich weiterer unselbstständiger geschriebener relativer Beweisverwertungsverbote bspw. § 160a Abs. 2 S. 1, 3 StPO.

2) Der Kernbereich als Auslöser eines absoluten Verwertungsverbot

Sofern eine nachgeordnete Prüfung ergibt, dass eine nach den §§ 100a-100c StPO erlangte Information dem Kernbereich zuzuordnen gewesen ist, normiert § 100d Abs. 2 StPO ein unselbstständiges geschriebenes Beweisverwertungsverbot. An dem hierdurch durch den Gesetzgeber normierten Ergebnis kann in keiner Weise durch entgegenstehende Interessen gerüttelt werden. Kernbereichsrelevante Daten sind nicht verwertbar.

a) Der Sozialbezug

Ob einem Sachverhalt ein höchstpersönlicher Charakter beizumessen ist, soll primär davon abhängen, in welcher Art und Intensität er die Sphäre anderer oder Belange der Gemeinschaft berührt.[1006] Je stärker der Sachverhalt dabei die Sphäre anderer oder die Belange der Gemeinschaft tangiert, desto eher erscheint eine Kernbereichsbetroffenheit ausgeschlossen. Dies würde bedeuten, dass der Kernbereich an dieser Stelle weniger von der betroffenen Person ausgehend, sondern vielmehr von bestehenden Berührungspunkten mit Dritten abhängig gemacht wird. Wieso allerdings an dieser Stelle zur Bestimmung des Kernbereichs nicht die formalen Kriterien, die das Bundesverfassungsgericht zur Bestimmung der negativen Kernbereichsprognose bemüht, herangezogen werden, ist nicht nachvollziehbar. Es greift zu kurz, wenn teilweise lediglich anhand dessen, in welcher Art und Intensität eine Information aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt[1007], abgeschätzt werden soll, ob diese dem Kernbereich zuzuordnen ist. Bei dieser Maßstabsbildung wird lediglich auf die Betroffenheit Dritter abgestellt. Die Frage nach der Höchstpersönlichkeit eines Verhaltens kann nicht an der Betroffenheit Dritter festgemacht werden, sondern muss sich primär aus dem Verhalten des Betroffenen ergeben. Dass durch das Abstellen auf die Betroffenheit Dritter an dieser Stelle eine Art Perspektivenwechsel vorgenommen wird überzeugt nicht. Daher ist sowohl hinsichtlich der Kernbereichsprognose im Rahmen der Beweiserhebung als auch hinsichtlich der Frage, ob der Kernbereich tatbestandlich eröffnet ist, maßgeblich die Thematik der Kommunikation, das Vertrauensverhältnis der miteinander Kommunizie-

1006 BverfGE 80, 367, 374; BverfGE 109, 279, 314.
1007 BverfGE 80, 367, 374; BverfGE 109, 279, 314 f.; BverfGE 113, 348, 391; BverfGE 124, 43, 69 f.; BverfGE 130, 1, 22.

renden, die Anzahl der Kommunizierenden oder auch auf die räumliche Situation des Gesprächs abzustellen.[1008] Aus einer Gesamtschau dieser Kriterien ergibt sich, ob die Kommunikation auch nach objektiven Kriterien einen derartigen Sozialbezug aufweist, dass diese womöglich nicht mehr als „höchstpersönliche" anzusehen ist. Insbesondere ist an dieser Stelle nochmals zu betonen, dass ein Straftatenbezug nicht generell einen derartigen Sozialbezug begründen kann, dass die Zuordnung zum Kernbereich nicht mehr möglich wäre.[1009]

b) Geheimhaltungswille

Neben der Höchstpersönlichkeit stellt der Wille des Betroffenen zur Geheimhaltung den zweiten Pfeiler der Kernbereichsdefinition dar.[1010] Dieser ist nicht berührt, wenn der Betroffene auf Geheimhaltung selbst „keinen Wert legt".[1011] Dies zeigt sich beispielsweise in der Art der Aufbewahrung einer Information oder der Wahl des Kommunikationspartners.[1012] Auch bei fahrlässig geringer Sicherung von vertraulichen Sachverhalten kann jedoch durchaus der Kernbereich einschlägig sein, weil eine fahrlässige Preisgabe des Grundrechtsschutzes und damit auch des Kernbereichsschutzes dem Grundgesetz fremd ist.[1013] Entsprechend hatte der BGH den Geheimhaltungswillen bejaht, obwohl die Beschuldigte zunächst die Wegnahme der Aufzeichnungen durch einen Dritten hingenommen hatte.[1014] In einem anderen Fall bewahrte der Beschuldigte die Notizen mit höchstpersönlichem Inhalt in einem unverschlossenen Raum auf. Hier sah der *BGH* dennoch einen Geheimhaltungswillen als gegeben an, da die Notizblätter erst nach gezielter Suche gefunden werden konnten.[1015] Im Rahmen der Bestimmung des Geheimhaltungswillens muss daher pri-

1008 *Gercke*, GA 2015, 339, 343 f.
1009 Vgl. § 5, A., I), 1), 2).
1010 BVerfG, Beschluss vom 10. Juni 2009 – 1 BvR 1107/09 -, Rn. 25 = teilweise in NJW 2009, 3357 ff.; BVerfG, Beschluss vom 18. April 2018 – 2 BvR 883/17 -, Rn. 38.
1011 BverfGE 80, 367, 374.
1012 *Dalakouras*, Beweisverbote und Intimsphäre, S. 204; *Delius*, Tagebücher als Beweismittel, S. 13.
1013 *Dammann*, Der Kernbereich der privaten Lebensgestaltung, S. 45; *Lorenz*, GA 1992, S. 254, 265; *Kamlah,* DÖV 1970, S. 361, 362.
1014 BGHSt 19, 325, 333.
1015 BGHSt 34, 397, 399.

mär darauf geachtet werden, ob die Aufzeichnungen frei zugänglich oder vor dem Zugriff besonders geschützt waren. Im Grundsatz wird davon auszugehen sein, dass je sorgloser die Art der Aufbewahrung oder die Auswahl des Gesprächsumfelds erfolgt, je geringer wird der feststellbare Geheimhaltungswille sein.[1016] Ein Sachverhalt gehört mangels Geheimhaltungswillens lediglich dann nicht zum Kernbereich, wenn der Betroffene ihn wissentlich und willentlich offenlegt und die Offenlegung nicht gegenüber einer Person des persönlichen Vertrauens geschieht. Letztlich ist das Kriterium des Geheimhaltungswillen jedoch eher als zusätzliches Kriterium neben der Intensität des Sozialbezuges heranzuziehen. Die Bedeutung dieses Kriteriums ist daher nicht zu hoch einzuordnen. Zwar ist der Geheimhaltungswille für die Eröffnung des Kernbereichs eine notwendige Bedingung, die jedoch in seiner praktischen Erfüllbarkeit keine hohen Maßstäbe verlangt. Praktisch wird die Eröffnung des Kernbereichs daher wohl kaum an einem fehlenden Geheimhaltungswillen scheitern.

3) Ungeschriebene Beweisverwertungsverbote

Soweit der Gesetzgeber keinerlei Regelungen geschaffen hat, wie mit einem Verstoß gegen eine Strafverfahrensnorm im Rahmen der Beweiserhebung umzugehen ist (zu denken wäre hier an einen Zugriff ohne Vorliegen der Voraussetzungen einer einschlägigen Ermächtigungsgrundlage, das Missachten der richterlichen Anordnungsbefugnis einer Eingriffsmaßnahme, das Unterbleiben einer Belehrung nach § 52 Abs. 3 StPO bzw. § 55 Abs. 2 StPO oder die Beschlagnahme trotz eines Beschlagnaheverbots nach § 97 StPO), hat dies weder ein automatisches Verwertungsverbot für die nicht rechtmäßig gewonnenen Beweisergebnisse zur Folge noch sind die hierzu heranzuziehenden Kriterien abschließend normiert. Heute herrscht dabei jedenfalls insoweit Einigkeit, dass nicht jede Verletzung einer Beweiserhebungsvorschrift zu einem Verwertungsverbot führe. Vielmehr sei die Frage der Verwertbarkeit eines fehlerhaft gewonnenen Beweismittels gesondert zu überprüfen.[1017]

1016 *Ellbogen*, NStZ 2001, 460, 464.

1017 BverfGE 122, 248, 272 f.; BVerfG, NJW 2011, 2417, 2418, Rn. 43 f.; BGHSt 44, 243, 249; BGHSt 51, 285, 289 f.; OLG Zweibrücken, StV 2019, 826, 828.

a) Rechtskreistheorie

Diese Überprüfung geschah in den Anfängen der Beweisverbotsthematik anhand der sog. Rechtskreistheorie deren Bezeichnung sich im Nachgang an die Grundsatzentscheidung des BGH zur Revisibilität eines Verstoßes gegen § 55 StPO[1018] in der Literatur abzeichnete.[1019] Der BGH hat seinen Ansatz ursprünglich gar nicht als Beweisverbotstheorie verstanden wollen wissen, sondern wollte damit lediglich eine Grenzziehung der Rügemöglichkeiten des Angeklagten im Rahmen der Revision leisten.[1020] Wohl auch, weil sich das Gericht insgeheim dennoch die Frage gestellt haben wird, ob ein Verwertungsverbot bestand und ob dessen Missachtung zu einem Verwertungsverbot führen könnte, wurde dieser durch den BGH gegründete Ansatz durch die Literatur zur Rechtskreistheorie fortentwickelt und so zu einem festen Bestandteil der Diskussion um die Entstehung eines unselbstständigen Beweisverwertungsverbotes.[1021] Inhaltlich soll dabei die „natürliche Stufung" unterschiedlicher Verfahrensnormen berücksichtigt werden. Handle es sich um eine übergeordnete, daher auf einer höheren Stufe stehende, Norm, die die rechtsstaatlichen Grundlagen des Verfahrens garantiere (u.a. § 169 GVG; §§ 22–27, 136a, 140, 338 StPO), komme es bei deren Missachtung nicht auf eine Verletzung des Rechtskreises des Beschuldigten an und es entstehe unabhängig davon ein Beweisverwertungsverbot.[1022] Erst auf der nächst tieferen Stufe soll untersucht werden, ob die Missachtung einer einfachen Beweiserhebungsvorschrift den Rechtskreis des Beschuldigten wesentlich tangiere oder ob sie für ihn nur von untergeordneter bzw. gar keiner Bedeutung ist.[1023] Ausgehend von dem Beweisverwertungsverbot als subjektives Recht des Beschuldigten soll stets zu fragen sein, ob lediglich das Recht des Staates oder das etwaiger Dritten beeinträchtigt ist oder der Verfahrensverstoß tatsächlich ein dem Rechtskreis des Beschuldigten zugehörendes Recht beeinträchtige. Im Ersten Fall bleibe das Ziel der Wahrheitserforschung vorranging, während lediglich im zweiten Fall von einem Beweisverwertungsverbot ausgegangen werden soll.[1024]

1018 BGH, NJW 1958, 557, 558.
1019 *Dencker*, StV 1995, 232.
1020 *Rogall*, JZ 2008, 818, 823.
1021 *Dencker*, StV 1995, 232, 234.
1022 BGH, NJW 1958, 557, 558.
1023 BGH, NJW 1958, 557, 558.
1024 *Trüg/Habetha*, NStZ 2008, 481, 483.

Kritisiert wird dieser Ansatz, da er nicht berücksichtige, dass der Zweck sämtlicher strafprozessualer Regelungen darin bestehe, dem Beschuldigten ein justizförmiges Verfahren und die Bindung des „strafenden Staates" an die StPO als Regelbuch der Strafverfolgung und Wahrheitsfindung zu garantieren.[1025] Eine Differenzierung strafprozessualer Vorschriften zwischen solchen, die dem Rechtskreis des Beschuldigten zuzuordnen sind und solchen, die seinem Rechtskreis nicht angehören, werde dem verfassungsrechtlich verankerten Anspruch des Beschuldigten auf ein gesetzmäßiges und justizförmiges Strafverfahren nicht gerecht.[1026] Wenn der Große Senat des BGH in seiner damaligen Grundsatzentscheidung zur Rechtskreistheorie jedoch der Überzeugung war, in § 55 StPO eine Vorschrift ausgemacht zu haben, die den Rechtskreis des Angeklagten nicht berührt, ist dem zwar zuzugestehen, dass das Auskunftsverweigerungsrecht aus § 55 StPO im Kern auf der Achtung der Persönlichkeit des Zeugen beruht. Nicht ganz von der Hand zu weisen, ist jedoch, dass der Zeuge in dem Fall, in welchem er von seinem Recht aus § 55 StPO nicht in Kenntnis gesetzt wurde, womöglich versucht sich oder nahe Angehörige mit einer wahrheitswidrigen Belastung des Angeklagten zu retten.[1027] Selbst wenn verschiedene Regelungen der StPO im Schwerpunkt nicht im Interesse des Angeklagten erlassen sind, sondern zum Schutze dritter Personen, welche in verschiedener Weise, bspw. als Zeuge, an der Wahrheitsfindung mitwirken,[1028] verdeutliche dies, dass jedenfalls mittelbar sämtliche Normen in ihrer Gesamtheit die Rechtsstaatlichkeit eines Verfahrens prägen und deren Einhaltung daher stets auch zum Zwecke der Wahrung der Rechte des Angeklagten geschehen muss. Wenngleich unter Zuhilfenahme der Rechtskreistheorie der klassische Fall einer unterbliebenen Belehrung des Zeugen nach § 55 StPO sachgerecht gelöst werden kann, so erscheint dennoch die kaum rechtssicher eingrenzbare und bestimmbare Weite des Rechtskreises des Beschuldigten problematisch. Für eine generelle Heranziehung zur Ermittlung eines unselbstständigen ungeschriebenen Beweisverwertungsverbotes ist die im Lichte der Revisibilität eines Verstoßes gegen § 55 StPO entwickelte Theorie folglich ungeeignet.[1029]

1025 *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 24; *Schmidt*, JZ 1958, 596, 597; *Hanack*, JZ 1971, 126, 127; *Dencker*, StV 1995, 232, 234.
1026 *Park*, Durchsuchung und Beschlagnahme, Rn. 388.
1027 *Hamm*, Die Revision in Strafsachen, S. 111.
1028 *Knauer/Kudlich* in: MüKo-StPO, § 337 StPO, Rn. 28.
1029 *Finger*, JA 2006, 529 531 f.; optimistischer *Bauer*, NStZ 1993, 2530, 2531.

b) Schutzzwecktheorie

Als Fortentwicklung der Rechtskreistheorie betrachtet auch die Schutzzwecklehre zunächst die verletzte Beweiserhebungsvorschrift.[1030] In der Literatur finden sich daran anknüpfend vor allem die auf *Grünwald* und *Rudolphi* zurückgehenden Ausgestaltungen. So soll für ein Verwertungsverbot Voraussetzung sein, dass trotz des Verfahrensverstoßes der durch die Norm intendierte Schutzzweck noch erreicht werden kann, sprich erst die nachfolgende Verwertung die Verletzung vollenden oder vertiefen würde.[1031] *Rudolphi* fordert, dass die Aufgabe der verletzten Verfahrensnorm gerade darin bestehe, den Einfluss bestimmter Beweismittel oder sonstiger Umstände auf das Urteil zu verhindern.[1032] Hierauf bezugnehmend gehen weitere Teile der Literatur davon aus, dass die Verwertung einer unter Verstoß gegen eine Beweiserhebungsvorschrift erlangten Erkenntnis ausscheide, wenn eine Verwertung nicht mit dem Schutzzweck der verletzten Norm zu vereinbaren ist. Denn der Schutzzweckgedanke will gerade ein solches verbotswidrig erlangtes Beweisergebnis von der Verwertung ausschließen.[1033] Insofern kann der maßgeblich von *Rudolphi* geprägte Maßstab, als der bei den Vertretern dieser Meinung herrschende angesehen werden. Kritiker bringen der Schutzzwecktheorie dagegen die gleichen Vorbehalte wie der Rechtskreistheorie entgegen.[1034] Auch sie beachte nicht hinreichend, dass der Angeklagte Anspruch auf ein prozessordnungsgemäßes und justizförmiges Verfahren habe und insofern auch ein Verstoß gegen Vorschriften, die nach der gesetzgeberischen Intension nicht dessen Schutz dienen ein Beweisverwertungsverbot nach sich ziehen können.[1035] Auch der BGH folgte, nachdem er sich 1974 von der Rechtskreistheorie abgewandt hatte, einem Ansatz, der der Schutzzwecklehre inhaltlich durchaus nahestand.[1036]

1030 Als „verbesserte Form der Rechtskreistheorie" bezeichnend *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 25.
1031 *Grünwald*, JZ 1966, 489, 492.
1032 *Rudolphi*, MDR 1970, 93, 99.
1033 *Beulke/Swoboda*, Strafprozessrecht, Rn. 705; *Paul*, NStZ 2013, 489, 490; *Beulke*, JURA 2008, 653, 656; *Jäger*, GA 2008, 473, 486.
1034 *Kühne*, Strafprozessrecht, Rn. 908.1.
1035 *Meyer-Mews*, JuS 2004, 126, 128.
1036 BGHSt 25, 325, 329 ff.

c) Abwägungslehre

Heute ist in der Rechtsprechung[1037] und Teilen der Lehre die Abwägungslehre herrschend[1038]. Mangels allgemeinverbindlicher Kriterien soll im Einzelfall durch eine umfassende Würdigung der widerstreitenden Interessen über die Verwertbarkeit entschieden werden. Ausgangspunkt ist die verfassungsrechtliche Pflicht des Rechtsstaates eine funktionstüchtige Strafrechtspflege zu gewährleisten.[1039] Zur Verwirklichung der rechtsstaatlichen Pflichten müssten ausreichende Vorkehrungen vorhanden sein, dass Straftäter nach Maßgabe der aktuellen Gesetzeslage verfolgt, abgeurteilt und tat- und schuldangemessenen Bestrafung zugeführt werden können.[1040] Ein Beweisverwertungsverbot bedeute folglich eine Ausnahme von diesem Grundsatz, zu der es – ein absolutes Beweisverwertungsverbot ausgenommen – nur aus übergeordneten wichtigen Gründen im Einzelfall kommen darf.[1041] Ein solcher Grund liege vor, wenn ein nach rechtsstaatlichen Grundsätzen geordnetes Ermittlungsverfahren durch einen Rechtsverstoß nachhaltig geschädigt wird.[1042] Im Kern stehen sich somit primär das Interesse des Staates an der Tataufklärung sowie das Interesse des Betroffenen an der Wahrung seiner Individualrechtsgüter gegenüber, wobei dem staatlichen Strafverfolgungsinteresse augenscheinlich ein „Vorsprung“ eingeräumt werden soll. Konkrete Anhaltspunkte für die bezeichnete Schädigung des rechtsstaatlichen Verfahrens können ein bewusst oder grob fahrlässiges Handeln der Ermittlungsbehörden entgegen der Verfahrensvorschriften,[1043] die Bedeutung der verletzten Verfahrensvorschrift für die Wahrung der Rechte des Beschuldigten,[1044] die (fehlende) Fairness des Verfahrens[1045] oder das besondere Gewicht des in Rede stehenden Rechts-

1037 Erstmals nahm der Senat im sog. Medizinalassistentenfall eine Abwägung vor, die letztlich zu Gunsten des Strafverfolgungsinteresse ausfiel, vgl. BGHSt 24, 125, 130; OLG Zweibrücken, StV 2019, 826, 828.

1038 *Greven* in: KK-StPO, vor § 94 StPO, Rn. 10; *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, S. 160 ff.; *Rogall*, ZStW 191979, 1, 31; *Meurer*, JR 1990, 389, 392.

1039 BVerfGE 33, 367, 383; BVerfGE 130, 1, 26; BVerfG, NJW 2009, 3225, Rn. 16.

1040 BVerfGE 33, 367, 383; BVerfGE 46, 214, 222; BVerfG, NJW 2009, 1469, 1474, Rn. 72.

1041 BGHSt 44, 243, 249, BGHSt 51, 285, 290, Rn. 20.

1042 BGHSt 51, 285, Rn. 21.

1043 BGHSt 51, 285, Rn. 28 f.; OLG Dresden, NJW 2009, 2149.

1044 BGH, NJW 2002, 975, 976; OLG Hamm, NStZ-RR 2006, 47.

1045 BGH, NStZ 2009, 519, Rn. 32 ff.; BGH NJW 2007, 3138, Rn. 30.

verstoßes sein[1046]. Gegen die Annahme eines Beweisverwertungsverbotes spreche insbesondere die Bedeutung der aufzuklärenden Straftat[1047] sowie die hypothetische Möglichkeit, dass die Ermittlungsbehörden das fragliche Beweismittel auch rechtmäßig hätten erlangen können (sog. hypothetischer rechtmäßiger Ersatzeingriff).[1048] Im Laufe der Jahre entwickelte sich in der höchstrichterlichen Rechtsprechung ein immer restriktiveres Verständnis hinsichtlich der Bejahung eines Beweisverwertungsverbotes. Ein solches soll erst dann angenommen werden, wenn eine Abwägung des öffentlichen Interesses an der Wahrheitsfindung mit den Beschuldigteninteressen einen nicht hinnehmbaren Eingriff in die Interessen des Betroffenen darstelle.[1049] Dieses restriktivere Verständnis – zu Lasten des Beschuldigten – begründet der BGH damit, dass das Anerkennen eines Beweisverwertungsverbotes schließlich eine „Korrektur der Strafprozessordnung"[1050] darstelle. Im Ergebnis bedeutet dies, dass gewissermaßen nur noch ein qualifizierter Verstoß zu einem Verwertungsverbot führen kann.[1051] Während die Flexibilität bei der Ermittlung eines Beweisverwertungsverbotes anhand der Abwägungslehre insbesondere von der Rechtsprechung sowie Teilen der Literatur als zielführendste Möglichkeit betrachtet wird[1052], kritisieren andere daran die fehlende Schärfe der Abwägungskriterien. Die Kritik gewinne ferner an Brisanz, da individuelle Vorstellungen der die Abwägung vornehmenden Richter, einheitliche und vorhersehbare Ergebnisse kaum zu gewährleisten vermögen.[1053] Es bestünde stets die Gefahr, mittels der „Abwägungslehre" Verfahrensverstöße im Sinne kriminalpolitisch wünschenswert erachteter Ergebnisse zu heilen.[1054]

1046 BGH, NJW 1986, 2261, 2264; OLG Hamm NStZ 2007, 355, Rn. 7.
1047 BGHSt 47, 172, 179; BGH, NStZ 2006, 236, Rn. 5.
1048 BVerfG, NStZ 2004, 216, 216.
1049 BGHSt 42, 170, 172; BGHSt 47, 172, 180.
1050 BGHSt 42, 170, 172.
1051 *Trüg*, Lösungskonvergenzen trotz Systemdivergenzen, S. 257 f.; *Trüg/Habetha*, NStZ 2008, 481, 485.
1052 *Rogall*, JZ 2008, 818, 824; *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, S. 163.
1053 *Grüner*, Revisibilität und Beweisverwertungsverbote, S. 39; *Dallmeyer*, Beweisführung im Strengbeweisverfahren, S. 216; *Müssig*, GA 1999, 119, 139 ff.; *Gaede*, JR 2009, 493, 502; *Grasnick*, NStZ 2010, 158, 159; *Neuber*, NStZ 2019, 113; *Löffelmann*, JR 2009, 10, 12; FS-Bemmann/*Amelung*, 505, 521 f.; diese Schwäche eingestehend auch *Rogall*, ZStW 1979, 1, 35.
1054 *Koch*, K&R 2004, 137, 138.

e) Stellungnahme

aa) Problematik der Abwägungslehre

Wenngleich den Strafgerichten zur Aufrechterhaltung einer effektiven Strafverfolgung darin zuzustimmen ist, dass nicht jeder Verstoß gegen Beweiserhebungsvorschriften ein strafprozessuales Verwertungsverbot nach sich ziehen kann, so muss dennoch sorgsam beachtet werden, nicht vorschnell auf die dargestellten Theorien zur Ermittlung eines Beweisverwertungsverbotes zurückzugreifen.[1055] Gerade bei absolut normierten Beweisverwertungsverboten ist die ein Beweisverwertungsverbot begründende Entscheidung bereits abschließend durch den Gesetzgeber getroffen. Würde an dieser Stelle dennoch in den Theorienstreit zur Ermittlung eines Beweisverwertungsverbotes eingestiegen, würde dies im Widerspruch zum freilich auch im Strafprozess geltenden Grundsatz der Gewaltenteilung aus Art. 20 Abs. 2 S. 2 GG stehen. Daher ist es auch nicht folgerichtig, eine mögliche Kernbereichsverletzung als „Abwägungsaspekt" im Rahmen der Abwägungslehre aufzufassen.[1056] Auf eine Einbeziehung einer Kernbereichsverletzung innerhalb der Abwägung, kann es überhaupt nicht mehr ankommen, da eine Kernbereichsverletzung bereits ein geschriebenes absolutes Beweisverwertungsverbot nach § 100d Abs. 2 StPO nach sich ziehen muss.

Allgemein fällt auf, dass mit der Abwägungslehre nicht die Begründung für die Verwertung eines rechtswidrig erlangten Beweismittels im Vordergrund steht, sondern trotz eines Rechtsverstoßes primär von der Verwertbarkeit ausgegangen wird und sodann lediglich sekundär nach einer möglichen Rechtfertigung für dessen Unverwertbarkeit gesucht wird.[1057] Damit wird nicht demjenigen dessen Handeln einen Verstoß gegen eine Beweiserhebungspflicht darstellt, das Begründungserfordernis einer notwendigen Verwertbarkeit des Beweisstückes auferlegt, sondern es soll eine Rechtfertigung für die Unverwertbarkeit geliefert werden,[1058] die eigentlich bereits in dem Verstoß gegen die Beweiserhebungsvorschrift gesehen

1055 *Beulke*, ZStW 1991, 657, 663 f.

1056 Insofern ist die Einordnung dieses Kriteriums in den Abwägungskanon abwegig, so gleichwohl *Hombrecher*, JA 2016, 457, 459.

1057 *Trüg/Habetha*, NStZ 2008, 481, 482.

1058 BVerfG, NJW 2011, 2417, Rn. 44; BGHSt 40, 211, 217; BGHSt 44, 243, 249; BGHSt 51, 285, Rn. 20; *Jahn*, Gutachten dt. Juristentag, C 68 (auf Grundlage seiner auf § 244 Abs. 2 StPO gründenden Beweisbefugnislehre, vgl. a.a.O.); *König/Harrendorf*, AnwBl. 2008, 566, 568.

werden könnte. Vergegenwärtigt man sich, dass sämtliche Vorschriften der StPO (deren Missachtung hier zu einem Beweisverwertungsverbot führen) ihren Ursprung in den Verfassungsprinzipien wie der Menschenwürde, dem Rechtsstaatsprinzip oder dem europarechtlichen Fair-Trial Grundsatz haben, so entspräche es lediglich verfassungsrechtlicher Grunddogmatik, dass der Staat, als dieses Recht verletzende Institution, gegenüber dem Betroffenen die Rechtfertigungslast zur Nutzung der hieraus gezogenen Früchte trägt. Mithin müsste primär von einer Unverwertbarkeit rechtswidrig erlangter Beweismittel ausgegangen werden und sodann untersucht werden, ob dies auch im konkreten Fall zu gelten hat.[1059]

Unabhängig davon darf die Abhängigkeit des Abwägungsergebnisses von den abwägenden Personen und damit zwangsläufig auch von rechtspolitischen Argumenten niemals die Lösung einer am Rechtsstaatsprinzip orientierten Beweisverbotslehre sein. Schon aus diesen Gründen müssen klare Maßstäbe und nicht eine Einzelfallabwägung den Ausschlag zur Verwertbarkeit oder Unverwertbarkeit eines Beweises geben.[1060] Es fragt sich, wie dieser Problematik Abhilfe geboten werden kann, ohne die stets unterschiedliche Bedeutung des konkreten Einzelfalles gänzlich aus den Augen zu verlieren. Möglicherweise könnte eine anderweitige Gewichtung der zu berücksichtigen Aspekte innerhalb der Abwägungslehre zu forcieren sein. Sollte ein rechtswidriges Beweismittel Eingang in das Urteil finden, so geschieht dies regelmäßig primär unter Verweis auf das hohe Strafverfolgungsinteresse.[1061] Die enorme Gewichtung dieses Kriteriums mag aus rechtspolitischen und gesellschaftspolitischen Gründen nachvollziehbar sein, da es einhellige Bestätigung finden dürfte, Straftäter einer das Unrecht derer Taten widerspiegelnden Strafen zuzuführen. Die starke Berücksichtigung der Tatschwere im Rahmen der Abwägung bringt jedoch mit sich, dass bei gewichtigen Straftaten diese stets zu Gunsten der Verwertbarkeit ausfällt. Die tatsächliche Abwägung verkommt regelmäßig zu einer bereits vorentschiedenen pro forma Abwägung.[1062] In letzter Konsequenz bedeutet dies gewissermaßen, dass – überspitzt formuliert – je schwerwiegender sich ein Delikt darstellt, je „unwichtiger" die Einhaltung der Verfahrensvorschriften ist.[1063] Allerdings kann sich unmittelbar aus

1059 Vgl. auch *Lucke*, HRRS 2011, 527, 531; FS-Wolter/*Kudlich*, 995, 1003 f.
1060 Zutreffend *Jugl*, Fair trial als Grundlage im Strafverfahren, S. 75.
1061 Vgl. etwa BGH, NJW 2003, 2034, 2035.
1062 Ähnlich auch *Fezer*, NStZ 2003, 625, 629.
1063 *Dencker*, Verwertungsverbote im Strafprozess, S. 97; *Jahn*, Gutachten dt. Juristentag, C1, C 61; a.A. *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, S. 167.

der Würde des Menschen tatsächlich nur das exakte Gegenteil ergeben: Je gewichtiger der dem Angeklagten gemachte Vorwurf (je höher daher die Strafandrohung ausfällt) desto wichtiger stellt sich Einhaltung der das gesamte Verfahren auszeichnenden Vorschriften dar. Schließlich wird der mit der Vollstreckung des Urteils einhergehende Eingriff in die Freiheitsrechte des Beschuldigten mit zunehmender Dauer der Freiheitsentziehung ebenso umso gewichtiger. Je gewichtiger aber der Eingriff in die (Freiheits-)Rechte des Betroffenen ausfällt, desto wichtiger ist, dass dieser auf einem rechtmäßig erlangten Fundament, in Form der dem Schuldspruch zugrunde liegenden Beweise, aufbaut.

bb) Ansatz Rehbeins

Einen neuen Weg schlägt *Rehbein* vor, die, wenn die Eingriffsbefugnis als solche bereits an der Schwere der Straftat anknüpft und daher bereits bestimmte Eingriffsschwellen normiert, auf das Kriterium der Schwere der Tat im Rahmen der Abwägung verzichten will.[1064] Würde die Schwere der Tat neben der Rechtfertigung des ursprünglichen Eingriffs auch maßgeblich zur Rechtfertigung der Verwertbarkeit herangezogen, würde dies eine Art der „Doppelverwertung" darstellen, die es entsprechend dem materiellen Recht nach § 46 Abs. 3 StGB auch prozessual nicht zu Lasten des Verdächtigen geben darf.[1065] Die Schwere der Straftat soll für die Verwertbarkeit nur dann von Relevanz sein, wenn eine bestimmte Schwere nicht bereits in der Beweiserhebungsvorschrift ihren Niederschlag gefunden hat.[1066] Erfreulich daran ist, dass mit diesem Vorschlag die mit der Gewichtung der Tatschwere als Hauptindikator des Strafverfolgungsinteresses einhergehende Problematik erkannt wurde. Die eingeschlagene Differenzierung vermag jedoch nicht gänzlich zu überzeugen. Der Umstand, dass eine Ermittlungsmaßnahme nicht auf Tatschwere rekurriert, vermag nicht auszuschließen, dass auch mittels einer solchen anlässlich einer erheblichen Straftat ermittelt wird. Im Rahmen der Abwägung käme man dann allerdings aufgrund unterschiedlicher zu berücksichtigender Kriterien zu einem fragwürdigen Auseinanderfallen der Abwägungsergebnisse. Ein Beweismittel das unter Missachtung der Anordnungsbefugnis beispielsweise nach § 100b StPO erlangte wurde, wäre womöglich nicht

1064 *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, S. 166.
1065 *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, S. 166 f.
1066 *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, S. 167.

verwertbar, da die Schwere der Tat außen vor zu bleiben habe, während das gleiche nach §§ 102, 110 Abs. 3, 94 StPO beschlagnahmte Beweismittel unter Berücksichtigung der erheblichen Straftat verwertbar wäre.[1067]

cc) Kriteriengewichtung im Rahmen der Abwägungslösung

Geboten erscheint es daher im Rahmen der gegen ein Verwertungsverbot sprechenden Kriterien die von der Rechtsprechung hervorgehobene Bedeutung der konkreten Straftat erheblich weniger stark zu gewichten.[1068] Stattdessen könnte das Kriterium eines hypothetisch-rechtmäßigen Ermittlungsverlaufes, dem im Rahmen der ständigen Rechtsprechung im Kanon der Abwägungsparameter eine verhältnismäßig geringe Bedeutung zukommt,[1069] stärker gewichtet werden. Dadurch würden den Umständen der rechtswidrigen Beweiserlangung im konkreten Fall besser Rechnung getragen werden, da die Verwertbarkeit nicht aufgrund einer schwe-

---

1067 Vgl. auch *Kelnhofe*r, Hypothetische Ermittlungsverläufe, S. 182 f.

1068 Zutreffend auch *Kassing*, JuS 2004, 675, 677 mit dem Verweis darauf, dass ein jeder Beschuldigter unabhängig von der Schwere des Tatvorwurfs unmittelbar aus dem Rechtsstaatsprinzip einen Anspruch auf Einhaltung der Verfahrensvorschriften hat; vgl. zu dieser Problematik auch das knappe bejahende Abstimmungsergebnis hinsichtlich einer Berücksichtigung des Schuldvorwurfes, Beschlüsse des 67. Dt. Juristentages, Band II, L. 66; den Umstand, dass die Rechtsprechung das Strafverfolgungsinteresse sehr stark in den Vordergrund rückt ebenfalls kritisch betrachtend, *Eder*, Beweisverbote, S. 89; FS-Roxin/*Wolter*, 1245, 1265.

1069 *Mayer*, jurisPR-StrafR 19/2018 Anm. 3; *Jäger*, JA 2016, 710, weisen darauf hin, dass in der Literatur umstritten sei, ob diese Rechtsfigur (neben der ihrer Heranziehung im Rahmen der Fernwirkung) auch bei unmittelbar erlangten Beweisen Anwendung finden kann. Tatsächlich beziehen sich die von diesen zitierten ablehnenden Stimmen in der Literatur jedoch ausschließlich auf die Frage, ob diese Figur auch im Falle der Verkennung des Richtervorbehalts zum Tragen kommen soll, vgl. *Ransiek,* StV 2002, 565, 570; *Krehl*, NStZ 2003, 461, 463 f.; *Mosbacher*, NJW 2007, 3686, 3687. Damit wird das Kriterium zur Entscheidungsfindung über die Verwertbarkeit eines unmittelbar erlangten Beweismittels jedoch nicht gänzlich abgelehnt. Vielmehr nennt *Wohlers*, StV 2008, 434, 440, Fn. 85, der durch *Jäger* als Gegner des hypothetischen Ersatzeingriffes im Rahmen der Ermittlung eines unselbstständigen Beweisverwertungsverbotes zitiert wurde, explizit den Gedanken an ein solches Vorgehen. Generell ablehnend gegenüber jeglicher Hypothesenbildung im Strafprozess dagegen jedenfalls *Jahn/Dallmeyer*, NStZ 2005, 297, 304; *Jahn*, Gutachten dt. Juristentag, C 77; die Zulässigkeit im Ergebnis von der Kategorie der Verfahrensvorschrift abhängig machend FS-Fezer/*Wohlers*, 311, 326.

ren Straftat gewissermaßen vorentschieden wäre, sondern entscheidend von möglichen alternativen rechtmäßigen Ermittlungsmöglichkeiten abhinge.[1070] Gleichzeitig würde die verfassungsrechtliche Forderung einer wirksamen Strafverfolgung im Verhältnis zu den Rechten des Betroffenen dadurch ausreichend priorisiert, dass in den Fällen, in denen die Strafverfolgungsbehörden ein Beweismittel auch auf legalem Wege hätten beschaffen können – solange es sich nicht um einen krassen Verstoß gegen die Menschenwürde handelt – kein Verwertungsverbot vorliegen würde. Auch im Übrigen sind der StPO hypothetische Erwägungen bekannt, wie die §§ 108, 161 Abs. 2 StPO belegen.[1071] Allerdings ist zuzugeben, dass sich sodann weitere schwierige Fragen der Bildung des Hypothesenmaßstabes stellen.[1072] Ferner ist zu beachten, dass es dem Kriterium des hypothetisch-rechtmäßigen Kausalverlauf an einer anerkannten einheitlichen dogmatischen Herleitung fehlt,[1073] womit es schwer fallen dürfte, dieses Kriterium zu einem tragenden im Rahmen der Abwägung zu bestimmen. Das Potential dieses Kriteriums im Kanons der Abwägungskriterien erscheint im Sinne einer am konkreten Einzelfall ausgerichteten Abwägung gleichwohl besser geeignet als der stetige Rekurs auf die besondere Schwere der Tat.

dd) Lösung

Um eine „Abwägung" anhand schwammiger Kriterien, die in Ermangelung klarer Leitlinien nicht einmal abschließend klären kann, welche Abwägungskriterien in welcher Gewichtung in den vorzunehmenden Abwägungsvorgang einzubeziehen sind,[1074] zu vermeiden, ist daher die Schutzzwecklehre gänzlich gegenüber der Abwägungslehre vorzuziehen. Zwar wird diese bereits teilweise als Kriterium im Rahmen der Abwägungslehre berücksichtigt, sofern sie sich jedoch einer schwereren Straftat gegenübersieht, wird sich ihre Wertung regelmäßig nicht durchsetzen können. Das Heranziehen der Schutzzwecklehre ermöglicht selbst bei einem ungeschriebenen unselbstständigen Beweisverwertungsverbot die Frage nach einem Beweisverwertungsverbot anhand des gesetzgeberischen

1070 *Schröder*, Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung, S. 105.
1071 *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, S. 170.
1072 *Jahn/Dallmeyer*, NStZ 2005, 297, 301; *Fezer*, NStZ 2003, 625, 629.
1073 verschiedene Möglichkeiten der Herleitung, vgl. *Abraham*, ZIS 2020, 120 ff.
1074 *Trüg/Habetha*, NStZ 2008, 481, 491; *Neuber*, Beweisverwertungsverbote im Strafprozess, S. 3.

Willens – der nicht zuletzt aus Gründen der Gewaltenteilung – Leitmotiv für sämtliche gerichtliche Entscheidungen sein muss, zu beantworten.[1075] Ein entscheidendes Merkmal der Schutzzwecklehre besteht darin, dass die ansonsten übliche Abwägung zwischen Verwertbarkeit und Unverwertbarkeit entfallen würde, da diese letztlich auch bei nicht absolut geschriebenen Beweisverwertungsverboten bereits durch den Gesetzgeber vorgenommen wurde.[1076] Würde die Abwägungslehre auch im gesamten Bereich der unselbstständigen Beweisverwertungsverbote gelten, so würde die Entscheidung des Gesetzgebers, der in der Normierung einer Beweiserhebungsvorschrift und der darin normierten Pflichten zur Begrenzung des Strafverfahrens, die jeweils in Frage stehenden gegenläufigen Interessen bereits abgewogen (und sich infolge dessen schließlich gerade für die Normierung einer allgemeinverbindlichen Begrenzung entschied) zum „bloßen Verhaltensvorschlag" zurückgestuft und damit „die Idee der Kodifikation als solche ad absurdum" geführt.[1077] Sofern der Schutzzweck bestimmt wurde, lässt sich somit ohne weitergehende Abwägung durch einen Blick, auf den durch den Gesetzgeber mittels der Kodifizierung verfolgten Zweck entscheiden, ob der vorliegende Verstoß im Rahmen der Beweiserhebung ein Beweisverwertungsverbot zur Folge haben muss. Hierdurch werden auch der Rechtsunsicherheit Vorschub leistenden Situationen vermieden[1078], in denen ansonsten womöglich derselbe Verfahrensverstoß bei der Beweisgewinnung hinsichtlich eines Betrugsverdacht zu einem Verwertungsverbot führen könnte, während bei Mordverdacht eine Verwertung zulässig wäre.[1079] Insbesondere kann mittels der Schutzzwecklehre eine Justizförmigkeit des Verfahrens gewährleistet werden, die auch bei erheblicheren Straftaten bestand hat. Indem die Schutzzwecklehre ferner ausschließlich anhand des Gesetzeszweckes zu ihren Ergebnissen kommt, wird zudem der der Abwägungslehre anhaftenden Beliebigkeit derer Ergebnisse abgeholfen.

Hier soll folglich vorgeschlagen werden, primär auf die Schutzzwecktheorie abzustellen, diese jedoch unter strengen Voraussetzungen – sofern mit dem Sinn des Schutzzweckes vereinbar – um die Figur des rechtmäßigen-hypothetischen Kausalverlauf zu ergänzen.[1080] Besteht die Möglichkeit

1075 *Beulke*, ZStW 1991, 657, 671 f.; *ders*., Jura 2008, 653, 656.
1076 *Trüg/Habetha*, NStZ 2008, 481, 483.
1077 *Wohlers*, StV, 2008, 434, 435; *Beulke*, Jura 2008, 653, 656.
1078 *Traub*, Verwertbarkeit von Selbstgesprächen, S. 33.
1079 *Fezer*, StV 1989, 290, 294.
1080 Ablehnend hinsichtlich hypothetischer Erwägungen im Rahmen der Schutzzweckzwecklehre, *Beulke,* ZStW 1991, 657, 674.

eines alternativen rechtmäßigen Ermittlungsverlaufes, der das entsprechende Beweismittel rechtmäßig hervorgebracht hätte, wird die normative Verknüpfung zwischen dem tatsächlich geschehenen, die Rechtswidrigkeit begründenden, (Verfahrens-)Fehler und dem Beweisergebnis aufgehoben, wodurch ein Beweisverwertungsverbot aus Schutzzweckgesichtspunkten nicht mehr erforderlich ist.[1081] Vorteilhaft im Vergleich zur bloßen Nutzung der Schutzzwecktheorie ist dies deshalb, da so ausgeschlossen wird, dass dem Betroffenen ein „Geschenk des Himmels" zuteilwerden könnte, indem das ihn belastende Beweismittel aus seiner Sicht glücklicherweise rechtswidrig erlangt wurde, obwohl es ohnehin auch auf rechtmäßigem Wege erlangt worden wäre.[1082] Zur Kombination dieser Figur mit der Schutzzwecklehre, soll jedoch für die Einhaltung dreier Weichenstellungen plädiert werden. Bezugspunkt des hypothetischen Alternativverlaufs muss stets die Erlangung des konkreten Beweismittels sein. An zweiter Stelle ist der Konkretisierungsgrad der Verlaufshypothese abschließend zu klären, bevor als dritte Weiche das Maß der Wahrscheinlichkeit der Beweismittelerlangung eingrenzt werden muss. Anhand des Bezugspunktes, dem Konkretisierungsgrad und dem Wahrscheinlichkeitsgrad, kann die Figur des hypothetischen Ersatzeingriffs rechtsstaatlich in einer Weise begrenzt werden[1083], die diese Figur sodann auch zum tauglichen Korrektiv im Rahmen der Schutzzwecklehre befähigt.

Erforderlich hierfür ist eine konkrete Hypothese anhand der Umstände des konkreten Falles.[1084] Gerade der BGH setzt aber, soweit er auf die hypothetisch rechtmäßigen Kausalverläufe zurückgreift, die Kriterien – ganz im Interesse einer Strafverfolgung – sehr niedrig an. Regelmäßig soll bereits die bloße abstrakt bestehende Möglichkeit, das entsprechende Beweismittel nach der Gesetzeslage auch legal erlangen zu können, genügen.[1085] Dem ist zu widersprechen. Es kann nicht maßgeblich sein, was nach dem Prozessrecht generell und abstrakt möglich gewesen wäre, sondern nur, was im Einzelfall angesichts der konkreten Sachlage als mög-

1081 *Wolter*, NStZ 1984, 275, 277; *Reichert-Hammer*, JuS 1989, 446, 450; *Schlüchter*, JR 1984, 517, 520; *Rogall*, NStZ 1988, 385, 388.
1082 Vgl. *Eisenberg,* Beweisrecht der StPO, Rn. 409.
1083 *Abraham*, ZIS 2020, 120, 126.
1084 *Flöhr,* Jura 1995, 131, 133; *Pelz*, Beweisverwertungsverbote und hypothetische Ermittlungsverläufe, S. 147 f.; *Roxin*, NStZ 1989, 376, 379.
1085 BGHSt 24, 125, 130; BGH, NStZ 1989, 375, 376; BGH, 1997, 294, 295; BGHSt 44, 243, 250; OLG Zweibrücken, NJW 1994, 810, 811; *Heghmanns*, ZIS 2016, 404, 410.

licher rechtmäßiger Ermittlungsverlauf tatsächlich in Frage kam.[1086] Demnach kann die der Hypothese zugrunde liegende Fragestellung nur lauten, ob zum Zeitpunkt des Rechtsverstoßes das entsprechende Beweismittel im konkreten Fall auch auf rechtmäßigem Wege noch erlangt worden wäre. Für die Praxis bedeutet dies, dass der fehlerhafte Kausalfaktor nicht schlicht durch eine theoretisch nach der Strafprozessordnung mögliche rechtmäßige Handlung ersetzt werden kann. Vielmehr muss die alternative rechtmäßige Handlung zum Zeitpunkt der rechtswidrigen Maßnahme bereits im konkreten Ermittlungsverfahren, daher aus den Ermittlungsakten erkennbar, angelegt gewesen sein.[1087] Dass es bereits dadurch – wie noch zu sehen sein wird – nur in seltenen Fällen zu einer Korrektur des Verwertbarkeitsergebnisses kommen wird, ist angesichts der Ausnahmefunktion dieses Korrektivs gerade wünschenswert. Daran anknüpfend ist zudem hinsichtlich des Beweismaßstabs innerhalb der konkreten Hypothesenbildung zu verlangen, dass die rechtmäßige Beweiserhebung sodann mit an Sicherheit grenzender Wahrscheinlichkeit erfolgt wäre.[1088] Andere verlangen dagegen nur eine einfache Möglichkeit der erfolgreichen Beweiserhebung[1089] oder, dass das rechtmäßige Auffinden des Beweismittels wahrscheinlicher gewesen wäre als das Gegenteil[1090]. Bezieht man in die Entscheidung mit ein, dass die Folge der Berücksichtigung eines hypothetisch-rechtmäßigen Kausalverlaufs die Verwertbarkeit eines im Sinne der Schutzzwecktheorie durch die gesetzgeberische Wertung als eigentlich unverwertbar eingeordneten Beweismittels ist, so kann die bloße Möglichkeit einer rechtmäßig Beweiserlangung nicht genügen.[1091] Wenn dieses

1086 *Rogall*, NStZ 1988, 385, 392.

1087 *Rogall*, NStZ 1988, 385, 392; *Reichert-Hammer*, JuS 1989, 446, 450; *Roxin* in: Jauernig/Roxin. Die Rechtsprechung des BGH, S. 97, mit Verweis auf die amerikanische inevitable discovery exception Rechtsprechung, die in dieser Frage in der Tat einen angemessen Weg weist, indem nur solche hypothetischen Kausalverläufe berücksichtigt werden, die in den Ermittlungen bereits angelegt waren; a.A.: *Pelz*, Beweisverwertungsverbote und hypothetische Ermittlungsverläufe, S. 154 f.

1088 *Roxin*, NStZ 1989, 376, 379; *Eisenberg*, Beweisrecht der StPO, Rn. 410; *Rogall*, NStZ 1988, 385, 392; *Wolter*, NStZ 1984, 276, 277; *Fezer*, JR 1991, 84, 87; *Eder*, Beweisverbote, S. 119; *Kasiske*, Jura 2017, 16, 22; *Pelz*, Beweisverwertungsverbote und hypothetische Ermittlungsverläufe, S. 153 f.; im Rahmen der Abwägungstheorie dazu auch BGH, NStZ 2016, 551, 552.

1089 BGHSt 32, 68, 71; BGHSt 34, 362, 364 f.

1090 *Schlüchter*, JR 1984, 517, 520; *Heghmanns*, ZIS 2016, 404, 411.

1091 *Schröder*, Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung, S. 118.

Korrektiv zur Verhinderung einer zu starken Beschneidung des Strafverfolgungsinteresse in Ausnahmefällen angewandt werden soll, darf jedoch auch bei Berücksichtigung der hypothetisch gesetzmäßigen Alternative der Schutz des Beschuldigten nicht einseitig vernachlässigt werden, weshalb entsprechend hohe Anforderungen an den Wahrscheinlichkeitsmaßstab zu stellen sind.[1092] Diesen hohen Anforderungen kann nur durch das Erfordernis einer mit an Sicherheit grenzenden Wahrscheinlichkeit genüge getan werden. Zusammenfassend sollte daher zur Ermittlung eines unselbstständigen ungeschriebenen Beweisverwertungsverbotes im Grundsatz auf die Schutzzwecklehre zurückgegriffen werden. Um allerdings „glückliche Fügungen" nicht zugunsten des Beschuldigten ausfallen zu lassen, soll – sofern mit der Eigenart der verletzten Norm vereinbar – auf einer zweiten Stufe unter Zuhilfenahme einer restriktiven Anwendung der Figur vom hypothetischen-rechtmäßigen Kausalverlauf ein Korrektiv angesetzt werden. Voraussetzung hierfür ist, dass bei einer konkreten Hypothese das konkrete Beweismittel zum damaligen Zeitpunkt unter Beachtung der bisher erlangten Erkenntnisse der Strafverfolgungsbehörden mit an Sicherheit grenzender Wahrscheinlichkeit auch rechtmäßig erlangt worden wäre. Unanwendbar bleibt das Korrektiv stets bei einem vorsätzlichen oder bewussten Missachten der Beweiserhebungsvorschriften durch die Strafverfolgungsbehörden.[1093] Solche eklatanten Rechtsverstöße durch Ermittlungsbeamte dürfen in einem Rechtsstaat nicht zuletzt deshalb nicht geduldet werden, um Umgehungsstrategien der Strafverfolgungsbehörden zu vermeiden.[1094] Nicht die Unverwertbarkeit eines in Folge eines solchen Verstoßes erlangten Beweismittels sondern der mit der Verwertung eines solchen kontaminierten Beweismittels einhergehende Vertrauensverlust in das rechtsstaatliche Ermittlungsverfahrens würde ein Effektivitätsverlust der Strafverfolgung befürchten lassen.[1095]

Dass der BGH aller Voraussicht nach das Entstehens eines unselbstständigen ungeschriebenen Beweisverwertungsverbotes weiter von der Abwägungsdoktrin abhängig machen wird, bleibt daher überaus kritisch zu betrachten. Insbesondere wäre eine Rückkehr des BGH zu einer von Schutz-

1092 *Schröder*, Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung, S. 121.

1093 So auch *Roxin*, NStZ 1989, 376, 379; FS-Roxin 2001/*Wolter*, 1141, 1161, Fn. 51; *Schneider*, NStZ – Sonderheft 2009, 46, 47.

1094 *Park*, Durchsuchung und Beschlagnahme, Rn. 393; *Schneider*, NStZ 2016, 553, 555.

1095 BGHSt 51, 285, 297; *Voßkuhle* in: Handbuch der Grundrechte, § 131, Rn. 114, Fn. 493.

zweckerwägungen getragen Entscheidung auch eine Rückkehr zu seiner eigentlichen Aufgabe, die zweifelsohne nicht in undurchsichtigen kasuistischen – vielmals rechtspolitisch geprägten – Abwägungsentscheidungen, sondern in der rechtskonformen Umsetzung und Aufrechterhaltung des gesetzgeberischen Willens zu sehen ist.

4) Konsequenzen für mögliche Konstellationen beim Zugriff auf einen Sprachassistenten[1096]

Die dargestellten Ansätze zur Entstehung eines unselbstständigen Beweisverwertungsverbotes erlangen in verschiedenen Szenarien schließlich auch im Rahmen der mithilfe von Smart Speakern und den hiermit verknüpften Sprachassistenten gewonnen Informationen Relevanz.

a) Fehlende richterliche Anordnung

Sowohl im Rahmen der Anordnung einer Maßnahme gem. §§ 100a ff. StPO als auch bei einer offenen Maßnahme gem. §§ 94 ff. StPO haben die Ermittlungsbehörden grundsätzlich eine richterliche Anordnung einzuholen, §§ 100e Abs. 1, 2, 105 Abs. 1 StPO. Im Falle der Aufzeichnung eines Telefongespräches, die bewusst ohne Einschaltung des zuständigen Richters erfolgte, ging der BGH von der Unverwertbarkeit der dadurch erlangten Beweise aus.[1097] Auch bei einem bewussten Zuwarten der Strafverfolgungsbehörden bis zu einem Zeitpunkt, zu dem eine richterliche Anordnung nicht mehr rechtzeitig zu erreichen war und sodann auf die Ausnahmeregelung „Gefahr im Verzug" abgestellt wurde, nahm der BGH eine Unverwertbarkeit der Beweise an, da die Voraussetzung zu Annahme von Gefahr im Verzug vorsätzlich herbeigeführt wurden und damit die richterliche Anordnungskompetenz untergraben werden sollte.[1098] Zur Korrektur soll in solchen Fällen der groben Verkennung der vorgeschriebenen Anordnungskompetenz auch ein Rekurs auf die Figur des hypothetisch rechtmäßigen Kausalverlaufs selbst dann nicht in Betracht kommen, wenn ein mit der Sache befasster Richter einen entspre-

1096 Bzgl. diverser Anwendungsbeispiele vgl. *Hombrecher*, JA 2016, 457 ff.
1097 BGHSt 31, 304, 306.
1098 BGHSt 51, 285, 292, Rn. 24, m.w.N.

chenden Beschluss erlassen hätte.[1099] Der Richtervorbehalt wäre sinnlos, wenn er vorsätzlich umgangen werden könnte und dies anschließend unter Zuhilfenahme der Figur des hypothetischen Ermittlungsverlaufs korrigiert würde. Vielmehr entstünde dann sogar ein Ansporn, die Ermittlungen, ohne die Einschaltung des Richters effizienter zu gestalten.[1100] Eine solche grobe Verkennung des Richtervorbehalts ist regelmäßig dann anzunehmen, wenn die Strafverfolgungsbehörden die Einholung einer richterlichen Anordnung nicht einmal erwogen haben oder die Strafverfolgungsorgane rechtsmissbräuchlich untätig zugewartet haben, bis die Voraussetzungen von Gefahr im Verzug tatsächlich vorlagen.[1101] Fraglich bleibt aber, wie mit einer aufgrund von Fahrlässigkeit fehlenden richterlichen Anordnung umgegangen werden soll.

Folgt man – wie hier vorgeschlagen – der Schutzzwecktheorie, ist in dem einen wie dem anderen Fall entscheidend, worin der Schutzzweck des Erfordernisses einer richterlichen Anordnung zu sehen ist. Dieser gründet auf dem Schutz der jedem Beschuldigten zustehenden Rechte, deren Einhaltung und Gewährleistung nicht allein dem die Maßnahme vornehmenden Beamten überlassen sein darf. Bereits an dieser Stelle müssen die durchgeführte Maßnahme von vornherein richterlich in einer angemessenen Weise begrenzt und kontrolliert werden.[1102] Mithin liegt der Sinn des Richtervorbehalts in einer präventiven richterlichen Kontrolle in Form eines gewissermaßen vorbeugenden Rechtsschutzes.[1103] Dieser Schutzzweck gilt gleich, ob es sich um einen vorsätzlichen oder nur fahrlässigen Verstoß gegen die Anordnungsvoraussetzung handelt. Unter Zugrundelegung der oben genannten Lösung muss daher auch das aus einem nur leichten Verstoß gegen die Anordnungskompetenz resultierende Beweisstück auf der ersten Ebene unverwertbar bleiben. Anschließend wäre allenfalls denkbar, mittels der Figur des rechtmäßigen-hypothetischen Ermittlungsverlaufs zu einer Unbeachtlichkeit des nur leichten Verfahrensverstoßes zu gelangen.[1104] Dabei ist jedoch zu bedenken, dass schwer vorstellbar ist, wie die hypothetisch mögliche Einhaltung von formellen Verfahrensvorschriften bereits im Ermittlungsverfahren angelegt gewesen sein soll. Hinzukommt, dass ohnehin nicht lediglich der fehlerhafte Kausalfaktor in Form der

1099 BGHSt 31, 304, 306.
1100 BGHSt 51, 285, 295 f., Rn. 29.
1101 *Brüning*, HRRS 2007, 250, 253 f.
1102 BVerfGE 42, 212, 220.
1103 A.A.: *Brüning*, HRRS 2007, 250, 252 f.; *Amelung/Mittag*, NStZ 2005, 614, 616.
1104 So *Roxin*, NStZ 1989, 376, 379, a.A.: *Jahn/Dallmeyer*, NStZ 2005, 297, 304.

unterbliebenen Anordnung durch ein rechtmäßiges Handeln ausgetauscht werden kann. Neben diesen Umständen ist angesichts der ebenfalls zu fordernden Höchstwahrscheinlichkeit einer hypothetisch rechtmäßigen Beweiserlangung zu beachten, dass mangels eindeutiger Prognostizierbarkeit richterlicher Entscheidungen auch diese nicht zu erreichen wäre.[1105] Schließlich kann eine richterliche Entscheidung nicht durch allgemeine Erfahrungssätze ersetzt werden.[1106] Aufgrund des Grundsatzes des gesetzlichen Richters aus Art. 101 Abs. 1 GG müsste die Hypothese ausschließlich auf dem Urteil des damals zuständigen Ermittlungsrichters beruhen. Daher müsste der damals zuständige Ermittlungsrichter notwendigerweise im entsprechenden Hauptverfahren als Zeuge gehört werden. Es werden jedoch berechtigten Zweifeln bestehen, inwiefern dieser nach teilweise mehreren Jahren zwischen Ermittlungsverfahren und Hauptverhandlung noch eine belastbare Aussage darüber treffen kann, wie er unter ausschließlicher Beachtung der damals bekannten Informationen entschieden hätte. Hinzu kommt, dass der gerichtlichen Anordnung insbesondere bei Maßnahmen, die den Schutzbereich des Art. 13 GG tangieren, gem. Art. 13 Abs. 2, 3, 4 GG eine ausdrücklich normierte verfassungsrechtliche Notwendigkeit zukommt, die keinen nachträglichen Korrekturen zugänglich ist[1107].[1108] Die Figur des hypothetisch-rechtmäßigen Kausalverlaufs ist nach dem Wesen des Richtervorbehalts daher auf diesen ohnehin nicht anwendbar. Insofern muss ein ohne Beachtung des Richtervorbehalts erlangtes Beweisstück – sofern nicht die Voraussetzungen der Gefahr im Verzug vorlagen – im Hinblick auf den stets zu beachtenden Verstoß gegen die richterliche Anordnungskompetenz unverwertbar sein.[1109] Indem der BGH ein

---

1105 *Beulke*, ZStW 1991, 657, 674.

1106 Mit *Ransiek*, StV 2002, 565, 570 könnte darüber lediglich dann diskutiert werden, wenn die Anordnung der Maßnahme die einzig rechtmäßige Entscheidung des Richters gewesen wäre, da sein Ermessen gewissermaßen auf Null reduziert war.

1107 *Park*, Durchsuchung und Beschlagnahme, § 2, Rn. 405; *Krekeler*, NStZ 1993, 263, 264.

1108 Letztlich muss jedoch auch einem lediglich einfachgesetzlich geregelten Richtervorbehalten bspw. nach § 100f Abs. 4, 100e Abs. 1, 3 StPO dieselbe grundrechtssichernde Wirkung wie den in Art. 13 GG verfassungsrechtlich normierten Richtervorbehalten zukommen. Insofern gilt folglich auch hinsichtlich deren Missachtung der gleiche strenge Maßstab, vgl. BVerfG, NJW 2007, 1345, Rn. 13; *Hüls*, ZIS 2009, 160, 167.

1109 *Wolter* in: SK-StPO, § 105 StPO, Rn. 79; *Fezer*, StV 1989, 290, 295; *Krehl*, JR 2001, 491, 494; *ders.*, NStZ 2003, 461, 463 f.; *Mosbacher*, NJW 2007, 3686, 3687; *Asbrock*, StV 2001, 322, 324; *Ransiek,* StV 2002, 565, 570; *Hüls*, ZIS 2009, 160,

solches Verwertungsverbot auf „Sonderfälle schwerwiegender Rechtsverletzungen“ beschränkt, wird dieser im Rahmen seiner Abwägungslehre bei nicht vorsätzlichen oder willkürlichen Verstößen entgegen dem Schutzzweck der Norm weiterhin zu einer Verwertbarkeit der so erlangten Informationen gelangen.[1110]

Gleichsam ist an dieser Stelle zu beachten, dass die in der Cloud gespeicherten Aufzeichnungen nicht nur durch eine Durchsuchung beim Betroffenen, sondern auch durch eine Beschlagnahme beim Dienstleistungsanbieter zu erlangen sind. Daher wäre zwar eine Verwertung der beim Betroffenen beschlagnahmten Audioaufzeichnungen nicht möglich, gleichwohl, wäre eine Verwertbarkeit der identischen Aufzeichnungen dann möglich, wenn zum Zeitpunkt der fehlerhaften Durchsuchung beim Betroffenen bereits eine Beschlagnahme der Audioaufzeichnungen unmittelbar beim Dienstleistungsanbieter konkret geplant war und folglich im Ermittlungsverfahren angelegt war. Sodann sind die zunächst beim Betroffenen beschlagnahmten Audioaufzeichnungen durch den begangenen Rechtsverstoß für den Prozess nicht „verbrannt“, sondern sind verwertbar, wenn die Audioaufzeichnungen alternativ durch die Beschlagnahme beim Dienstleistungsanbieter mit an Sicherheit grenzender Wahrscheinlichkeit erlangt worden wären. Dabei ist auch nicht zu befürchten, dass die Strafverfolgungsbehörden sich durch das Vorbehalten alternativer Ermittlungsvorgänge im Ermittlungsverfahren ein Sicherheitsnetzes hinsichtlich möglicher Verstöße spinnen könnten. Zum einen werden die Strafverfolgungsbehörden von der Rechtmäßigkeit ihres Vorgehens überzeugt sein und folglich die Notwendigkeit eines solchen doppelten Sicherheitsnetzes gar nicht für erforderlich halten. Zum anderen käme dieses Korrektiv ohnehin bereits nicht zur Anwendung, wenn die Ermittlungsbeamten wider Erwarten den Rechtsverstoß bei der Beweiserhebung in der vermeintlichen Sicherheit auf hypothetische, die Verwertbarkeit sichernde, Erwägungen bewusst in Kauf nähmen. Ferner müssen die alternativen Ermittlungsansätze

---

169; im Grunde auch *Wohlers*, StV 2008, 434, 440, der in Fn. 85 jedoch erwägt, ob eine Heilung durch den hypothetischen Ersatzeingriff erfolgen könnte.

1110 BGHSt 51, 285, 291; hierfür spricht auch, dass der BGH ausführt, dass „dem Aspekt eines möglichen hypothetisch rechtmäßigen Ermittlungsverlaufs […] bei […] *solcher* Verkennung des Richtervorbehalts keine Bedeutung zukommen [kann]“ (Hervorhebung durch Verfasser), wobei er sich auf eine bewusste und willkürliche Verkennung des Richtervorbehalts bezog und daher anzunehmen ist, dass dies bei einem bloß fahrlässigen Verstoß unterschiedlich zu bewerten wäre, BGHSt 51, 285, 296; BGH, StV 2016, 539, 540; in die gleiche Richtung tendiert *Amelung*, NJW 1991, 2533, 2536 f.

im Zeitpunkt des Rechtsverstoßes hinreichend konkret im Ermittlungsverfahren angelegt sein, sodass beispielsweise der bloße in der Ermittlungsakte festgehaltene Gedanke einer solchen Alternative nicht genügt.

b) Fehlende Ermächtigungsgrundlage

Denkbar erscheint auch, dass der Zugriff angesichts der dargestellten potenziellen Möglichkeiten auf eine falsche Ermächtigungsgrundlage gestützt wird. Zu erinnern ist an § 100a StPO, der – nach der hier vertretenen Auffassung – keinen tauglichen Gesetzesvorbehalt normiert. Es bleibt zu fragen, inwiefern dies die Verwertbarkeit der dadurch erlangten Informationen hindert. Dass jedenfalls eine fehlende Ermächtigungsgrundlage zu einem Beweisverwertungsverbot führt, entschied der BGH im Entführungsfall „Schleyer", indem er die heimliche Aufnahme eines Gespräches außerhalb der förmlichen Vernehmung zwecks Stimmenvergleich mangels strafprozessualer Ermächtigungsgrundlage als unverwertbar einordnete.[1111] Auch bei Zugrundelegung der Schutzzwecktheorie wäre in diesem Fall zu konstatieren gewesen, dass das Erfordernis einer einschlägigen Ermächtigungsgrundlage gerade schrankenlose Eingriffe in die Rechte des Betroffenen verhindern soll. Ohne einschlägigen Gesetzesvorbehalt erlangte Informationen müssen daher unverwertbar sein. Kennt die StPO bereits keine wenigstens theoretisch einschlägige Ermächtigungsgrundlage, kann folglich von vornherein auch nicht die Möglichkeit einer hypothetisch rechtmäßigen Beweiserlangung auf zweiter Stufe zum Zeitpunkt der Verwertung in Betracht gezogen werden.

c) Falsche Ermächtigungsgrundlage

Daran anknüpfend stellt sich die Frage, wie zu verfahren ist, wenn die Überwachung der aktiven Nutzung eines Sprachassistenten, nach hier vertretener Auffassung, zwar nicht nach § 100a StPO erfolgen kann, stattdessen aber – wie festgestellt – rechtmäßig im Zuge einer Live-Online-Überwachung nach § 100b StPO. Das gleiche Problem stellt sich bei einer Durchsuchung, die fälschlicherweise auf die falsche Eingriffsnorm (§ 102 StPO oder § 103 StPO) gestützt wurde. Im Unterschied zum Fall einer gänzlich fehlenden Ermächtigungsgrundlage kennt die StPO in die-

1111 BGHSt 34, 39, 43.

sen Fällen eine Ermächtigungsgrundlage, auf die die Ermittlungsmaßnahme hätte gestützt werden können. Ob der Fall einer tatbestandlich nicht einschlägigen Ermächtigungsgrundlage analog zum Fall einer gänzlich fehlenden Ermächtigungsgrundlage behandelt werden muss, hängt maßgeblich vom Verhältnis und den Voraussetzungen der entsprechenden alternativen Ermittlungsmöglichkeiten ab.

aa) §§ 102, 103 StPO

Sofern bei einer Durchsuchung nach § 102 StPO, die eigentlich auf § 103 StPO zu stützen gewesen wäre, ein Beweismittel erlangt wird, soll dieses nicht verwertet werden dürfen, da ansonsten die strengeren Maßstäbe des § 103 StPO missachtet würden.[1112] Praktisch relevant wird dies beispielsweise dann, wenn gegen eine Person fälschlicherweise ein Anfangsverdacht i.S.d. § 102 StPO bejaht wird, obwohl ein solcher nicht vorlag und die Durchsuchung folglich nur unter den strengeren Voraussetzungen des § 103 StPO hätte erfolgen dürfen.[1113] Insofern soll das Erfordernis bestimmter tatbestandlicher Voraussetzungen den betroffenen Dritten davor bewahren, dass der ihm grundrechtliche gewährte Schutz nicht ohne das Vorliegen tatsächlicher Anhaltspunkte eingeschränkt wird. Erfolgt diese Einschränkung obwohl tatbestandliche Voraussetzungen nicht vorlagen, läuft dies dem von § 103 StPO ausgehenden Schutz entgegen, womit die erlangten Informationen nicht verwertbar wären.

Zu denken ist erneut an eine Unbeachtlichkeit aufgrund eines rechtmäßigen hypothetischen Ermittlungsverlaufes. Es ist abermals zu fragen, ob die Durchsuchung im konkreten Fall ihre Rechtsgrundlage in § 103 StPO hätte finden können, deren Voraussetzungen vor ihrer Durchführung vorgelegen hätten und folglich mit an Sicherheit grenzender Wahrscheinlichkeit auch eine solche Anordnung ergangen wäre.[1114] Da die §§ 102, 103 StPO im Kern die gleiche Maßnahme zu Gegenstand haben, würde in diesem Fall ein hypothetischer Wechsel der Ermächtigungsgrundlage nicht zu einem identitätsverändernden Austausch der Ermittlungsmaßnahme führen. Entscheidend ist somit, ob die zum Zeitpunkt der Durchsuchung beim vermeintlichen Verdächtigen vorliegenden Tatsachen, auch

1112 *Ciolek-Krepold*, Durchsuchung und Beschlagnahme im Wirtschaftsstrafverfahren, Rn. 101.
1113 *Krekeler*, NStZ 1993, 263, 265.
1114 So *Krekeler*, NStZ 1993, 263, 265.

eine Durchsuchung bei einem Dritten nach § 103 StPO legitimiert hätten und insofern auch diese Durchsuchung bereits im Ermittlungsverfahren angelegt war. Einfacher ist die Lösung im umgekehrten Fall, in dem eine Anordnung auf § 103 StPO gestützt wurde, obwohl diese auch nach § 102 StPO hätte ergehen können. In diesem Fall wird mit an Sicherheit grenzender Wahrscheinlichkeit davon ausgegangen werden können, dass bei einer durchgeführten Durchsuchung gem. § 103 StPO erst Recht die Möglichkeit der geringeren Voraussetzungen unterworfenen Durchsuchung nach § 102 StPO bereits im Ermittlungsverfahren angelegt war.[1115]

bb) § 100a StPO

Anders stellt sich dies bei einer Überwachung der Sprachassistenznutzung auf Grundlage des § 100a StPO dar. Der dem Vorbehalt des Gesetzes in solchen Fällen immanente Schutzzweck würde eine Unverwertbarkeit auf diese Weise erlangter Informationen erfordern. Zwar gäbe es in Form des § 100b StPO auch hier eine alternative Ermächtigungsbefugnis, doch vermag dies an der Beachtlichkeit des rechtswidrigen Beweiserhebung nicht zu ändern. Zum Zeitpunkt der rechtswidrigen Aufzeichnung der belastenden Audioaufzeichnung war es aus faktischen Gründen nicht mehr möglich, diesen flüchtigen Gesprächsausschnitt hypothetisch noch auf andere Weise zu erlangen. Das Korrektiv des hypothetisch rechtmäßigen Ermittlungsverlaufes soll die Strafverfolgungsbehörden gerade nicht in die Vergangenheit zurückversetzen, um einen hypothetischen, die Identität der Ermittlungsmaßnahme ändernden Austausch der Ermächtigungsgrundlage zu ermöglichen, sondern lediglich fragen, ob die rechtswidrig erhobene Audioaufzeichnung – hätte es die rechtswidrige Maßnahme nicht gegeben – auch auf einem alternativen rechtmäßigen Wege noch erlangt worden wäre. Dies ist aufgrund der Flüchtigkeit der Aussage zu verneinen. Selbst wenn man einen solchen hypothetischen Austausch der Ermächtigungsgrundlage aber mit einer abstrakten Sichtweise zulassen wollte, könnte nicht mit der notwendigen „an Sicherheit grenzenden Wahrscheinlichkeit" davon ausgegangen werden, dass eine alternative Anordnung nach § 100b StPO ergangen wäre und so die entsprechende Audioaufzeichnung auch rechtmäßig erlangt worden wäre. Schließlich ist der über die Anord-

1115 Vgl. im Ergebnis auch BGHSt 28, 57, 60; KK/*Bruns* § 103 StPO, Rn. 3; *Köhler* in: Meyer-Goßner/Schmitt, § 103 StPO, Rn. 1; *Ciolek-Krepold*, Durchsuchung und Beschlagnahme im Wirtschaftsstrafverfahren, Rn. 102.

nung im Ermittlungsverfahren entscheidende gesetzliche Richter bei einer Maßnahme nach § 100a StPO im Vergleich zu § 100b StPO personenverschieden. Während gem. § 100eAbs. 1 StPO n.F. über eine Anordnung nach § 100a StPO der zuständige Ermittlungsrichter entscheidend,[1116] obliegt diese Entscheidung bei einer Online-Durchsuchung gem. § 100e Abs. 2 StPO einer in § 74a Abs. 4 GVG genannten Kammer des Landgerichts. Die hierfür zuständige Staatsschutzkammer entscheidet regelmäßig in der Besetzung mit drei Berufsrichtern, sodass der gesetzliche Richter des Beschuldigten bei einer Anordnung nach § 100b StPO im Unterschied zu einer Anordnung nach § 100a StPO aus drei Richtern besteht.[1117] Aufgrund der unterschiedlichen Zuständigkeit kann die mit an Sicherheit grenzende Wahrscheinlichkeit einer entsprechenden Anordnung – ungeachtet der ohnehin erheblich größeren Eingriffsintensität einer Anordnung nach § 100b StPO – nicht dadurch hergeleitet werden, dass wenn bereits eine Maßnahme nach § 100a StPO angeordnet wurde, auch eine solche nach § 100b StPO angeordnet worden wäre. Bei einem Zugriff auf einen Sprachassistenten nach § 100a StPO sind die dabei gewonnen Beweismittel daher unverwertbar.

II) Selbstständige Beweisverwertungsverbote

Selbst wenn die Beweiserhebung schließlich im Einklang mit den strafprozessualen Ermächtigungsvorschriften erfolgte, bleibt möglich, dass faktisch Informationen vernommen wurden, die aus rechtsstaatlichen Gründen der Verwertung entzogen bleiben müssen. Bezüglich der selbstständige Beweisverwertungsverbote besteht Einigkeit dahingehend, dass diese aus den Grundrechten herzuleiten sind.[1118] Ebenfalls hinsichtlich selbstständiger Beweisverwertungsverbote relevant sind die Situationen, in denen es gänzlich an einer staatlichen Beweiserhebung fehlt, da die einschlägigen Beweise überhaupt nicht durch den Staat selbst, sondern durch Private erlangt wurden.[1119]

1116 *Graf* in: BeckOK-StPO, § 100e StPO, Rn. 4.
1117 *Huber* in: BeckOK-GVG, § 74a GVG, Rn. 6.
1118 *Eisenberg,* Beweisrecht der StPO, Rn. 362, m.w.N.
1119 *Dautert*, Beweisverwertungsverbote und ihre Drittwirkung, S. 11; *Volk/Engländer,* GK StPO, § 28, Rn. 35.

1) Grundrechtsbeeinträchtigungen beim Zugriff auf Sprachassistenten

Voraussetzung für ein selbstständiges Beweisverwertungsverbot ist eine mit der Verwertung einhergehende, jedoch durch die mit der Verwertung verfolgten Ziele, nicht zu rechtfertigende Grundrechtsbeeinträchtigung. Insofern stellt sich die vorgelagerte Frage, inwiefern die Nutzung eines Sprachassistenten durch die Verfassung überhaupt geschützt ist.

a) Art. 13 GG

Art. 13 GG tritt insbesondere dann in den Vordergrund, wenn es im Rahmen einer Maßnahme gem. § 100c StPO zu einer Überwachung des Beschuldigten kommt. Daneben könnte Art. 13 GG jedoch auch bei einer Live-Überwachung gem. § 100b StPO zum Tragen kommen. Maßgeblich abhängig ist dies vom durch Art. 13 GG gewährten Schutzumfang.

aa) Schutzbereich Art. 13 GG

Der Schutzbereich aus Art. 13 Abs. 1 GG umfasst die Wohnung als Raum der individuellen Persönlichkeitsentfaltung sowie in ihrer fundamentalen Funktion dem Einzelnen ein Heim zu bieten.[1120] Mittels dieser gewährleisteten Rückzugmöglichkeit soll der Grundstein für ein persönliches und – dies wird noch zu klären sein – möglicherweise auch geschäftliches Verhalten gelegt werden. Schutzauftrag des Art. 13 Abs. 1 GG ist es dabei das fremde – zuvörderst staatliche – Eindringen in diesen Bereich zu verhindern. Dem Bürger soll und muss ein Recht zustehen, alleine und in Ruhe gelassen zu werden.[1121] Der Grundrechtsträger muss darüber entscheiden können, welche Informationen aus seinem persönlichen Rückzugsbereich Dritten Personen zugänglich sein sollen.[1122] Entscheidend für die Dispositionsbefugnis und damit auch für die Hürde eines staatlichen Zugriffs ist, welche Bereiche unter den Wohnungsbegriff des Art. 13 GG fallen.

1120 BVerfGE 120, 274, 309 f.; *Papier* in: Maunz/Dürig-GG, Art. 13 GG, Rn. 1; *Hufen*, Grundrechte, § 15, Rn. 3.

1121 BVerfGE 32, 54, 75; BVerfGE 42, 212, 219; BVerfGE 51, 97, 110; BVerfGE 103, 142, 150 f.; *Kingreen/Poscher*, Grundrechte, Rn. 1004.

1122 *Hermes* in: Dreier-GG, Art. 13 GG, Rn. 12.

(1) Weite Auslegung

Im Anschluss an eine richtungsweisende Entscheidung des Bundesverfassungsgerichts vertritt die Rechtsprechung und sich daran anschließend ein Großteil der Literatur eine sehr weite Auslegung des Wohnungsbegriffes.[1123] Daraus folge, dass auch Arbeits-, Betriebs- und Geschäftsräume von Art. 13 GG umfasst seien. Zur Begründung wird zum einen ein historischer Rekurs bemüht, da bereits Art. 6 der preußischen Verfassung von 1850 und Art. 115 WRV von einem weiten Wohnungsbegriff ausgegangen sind.[1124] Ferner spreche der Sinn und Zweck die Privatsphäre, die freie Entfaltung der Persönlichkeit umfassend zu schützen für eine weite Auslegung. Ein persönlichkeitsrelevantes Verhalten wird ebenso in Arbeits- oder Geschäftsräumen vorkommen.[1125] Der teilweise unternommene Versuch einer Begrenzung des Schutzbereiches hin zu einem engen Wohnungsbegriff, der der umgangssprachlichen Bedeutung des Begriffes „Wohnung" folgend lediglich Räume zum privaten Rückzug schützen wolle[1126], fuße auf einer fehlerhaften Priorisierung des Wortlauts.[1127] Insofern würde sowohl die seit mehr als einem Jahrhundert unverändert gebliebene weite Auslegung als auch die geschichtlichen Erfahrungen, die die Anfälligkeit gerade dieses Lebensbereichs gegenüber Eingriffen der öffentlichen Gewalt zeige, verkannt.[1128] Ein Blick in die Entwicklung der Rechtsprechung zeigt zudem, dass zwischen dem Schutzumfang als solchem und der Intensität und Qualität dieses Schutzumfanges zu differenzieren ist. Die Weite des Schutzbereiches hat zur Folge, dass an die Zulässigkeit von Eingriffen unterschiedlich hohe Anforderungen zu stellen sind. In Abhängigkeit der Nähe eines Ortes zur räumlichen Privatsphäre, werde lediglich bei Räumen, in denen sich das Privatleben im engeren Sinn abspielt, das Schutzbedürfnis vollumfänglich zum Tragen kommen. Wohingegen für reine Betriebs-, Geschäfts- oder Arbeitsräumen der staatlich zuerkannte Schutz in Abhängigkeit, von der nach außen gewährten Offenheit zurückgeht.[1129] Auch bei Zugrundelegung eines weiten Begriffsverständnis wird für den Schutz des Art. 13 GG jedenfalls ein Mindestmaß an physischer

1123 BVerfGE 32, 54; *Gornig* in: v. Mangoldt/Klein/Starck, Art. 13 GG, Rn. 34.
1124 BVerfGE 32, 54, 69.
1125 BVerfGE 32, 54, 70 f.
1126 *Stein/Frank*, Staatsrecht, S. 293; *Battis*, JuS 1973, 25, 29 f., *Behr*, NJW 1992, 2125, 2126.
1127 BVerfGE 32, 54, 71 f.
1128 BVerfGE 32, 54, 71 f.
1129 BVerfGE 97, 228, 266.

und informationeller Abschottung aufweisender Bereich privaten Lebens und Wirkens gefordert.[1130] Dennoch werden unter einem solch weiten Begriffsverständnis selbst Einkaufszentren oder gar Sportstadien als Wohnung i.S.d. Art. 13 GG angesehen.[1131]

(2) Enge Auslegung

Einer strikten Wortlautorientierung entsprechend sollen bereits all jene Bereiche nicht vom Schutzbereich umfasst werden, die keine Wohnung im klassischen Sinne darstellen, mithin nicht zum dauerhaften Aufenthalt von Menschen bestimmt sind und daher nicht der privaten Lebensführung dienen. Geschäftsräume wie Banken oder Supermärkten fehle es an dieser Eigenschaft ebenso wie einem einfachen Besprechungszimmer.[1132] Sodann bliebe für sämtliche Betriebs- und Geschäftsräume allein der Schutz des Art. 2 Abs. 1 GG.

(3) Vermittelnde Ansichten

Vermittelnde Autoren wollen zwar grundsätzlich einen weiten Schutzbereich anerkennen, diesen jedoch im konkreten Fall von weiteren Voraussetzungen abhängig machen. So soll der Schutzbereich des Art. 13 GG nicht für Räumlichkeiten gelten, wenn über den Zugang zu diesen Räumen nicht individuell entschieden werden kann.[1133] Der Art. 13 GG zugrunde liegende Schutz der räumlichen Privatsphäre bestehe jedenfalls dann, wenn Räume der Öffentlichkeit durch physische Grenzen entzogen sind. Der Grundrechtsträger muss die nach außen abgeschlossene Räumlichkeit faktisch gegenüber der Öffentlichkeit beherrschen.[1134] Danach wäre beispielsweise ein Angestellter in seinem Büro oder etwa der Besprechungsraum einer Bank oder Kanzlei, die nicht ohne individuelle Prüfung dem Publikumsverkehr geöffnet sind, vom Schutzbereich umfasst. Im Unterschied zur weiten Rechtsprechung des Bundesverfassungsgerichts

1130 So die Kasuistik des BVerfG zum Wohnungsbegriff zusammenfassend *Gornig* in: v. Mangoldt/Klein/Starck, Art. 13 GG, Rn. 20; *Koranyi*, JA 2014, 241, 242.
1131 Vgl. BVerfGE 97, 228, 265; *Epping*, Grundrechte, Rn. 666.
1132 *Stein/Frank*, Staatsrecht, S. 293; *Battis*, JuS 1973, 25, 29 f., *Behr*, NJW 1992, 2125, 2126.
1133 *Ruthig*, JuS 1998, 506, 510; *Epping*, Grundrechte, Rn. 668.
1134 *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, S. 186.

wäre dagegen die Schalterhalle der Bank oder der Einkaufsbereich des Supermarktes, die einem freien Zugang unterliegen und folglich nicht die Atmosphäre von Vertraulichkeit vermitteln, nicht geschützt.[1135] Diese zusätzlichen Voraussetzungen stellen sicher, dass die grundrechtlich geschützten Räumlichkeiten entweder durch ein Vertraulichkeitsverhältnis zwischen Beschäftigten und Publikum oder dem persönlichem Rückzug geprägt sind. Derjenige der Geschäftsräume ohne Differenzierung öffnet, kann schlussendlich nicht einwenden, dass der Staat dort keinen Zugang haben dürfe.[1136]

(4) Stellungnahme

Betrachtet man Art. 13 GG im Lichte der gängigen Auslegungsmethoden, so stehen die Wortlautauslegung, die für ein enges Verständnis streitet, und die historische Auslegung, welche einem weiten Verständnis folgt, in einem offensichtlichen Widerspruch. Daneben wird allerdings sowohl eine systematische als auch eine teleologische Betrachtungsweise für eine weitere Auslegung streiten. Im Gesamtkonzept der Grundrechte sind diese grundsätzlich nicht anhand des gewöhnlichen Sprachgebrauchs, sondern anhand des durch sie verfolgten Zweckes auszulegen. Dieser liegt im weitesten Sinne bei einem jedem Grundrechte in der Wahrung der Persönlichkeit des Bürgers durch die Gewährung eines Bereiches frei von staatlicher Einflussnahme.[1137] Sei dies durch das Recht offen seine Meinung zu äußern, frei seine Religion auszuüben oder seine Meinung im Rahmen einer Versammlung kundzugeben, so ist dies im Rahmen des Art. 13 GG das Recht an bestimmten Örtlichkeiten frei von der Beobachtung durch Dritte zu sein. Dieses zeitgleich ein Verlangen des Einzelnen darstellendes Recht kann nicht abrupt mit dem Verlassen der Wohnung im engsten Sinne enden. Gerade angesichts dessen, dass viele Berufstätige teilweise mehr als die Hälfte des Tages außerhalb der Wohnung im klassischen Sinne verbringen, muss auch das eigene Büro in einer Bank, Kanzlei oder einem Unternehmen oder das für ein vertrauliches Gespräch aufgesuchte Besprechungszimmer unter den Schutz des Art. 13 GG fallen. Letztlich werden dabei aber sowohl die weite Ansicht des Bundesverfassungsgerichts als auch die vermittelnden Ansichten in der Regel zu identischen Ergebnis-

1135 *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, S. 186.
1136 *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, S. 187.
1137 Vgl. zum Schutzzweck der Grundrechte, § 4, B), I), 2), b), cc), (2).

sen kommen. Während die weite Auffassung zwar nicht auf Ebene des Schutzbereichs, jedoch unmittelbar danach im Rahmen des tatsächlich bestehenden Gewährleistungsumfang ein Korrektiv in Form der unterschiedlich Intensität des Gewährleistungsumfangs ansetzt, will die vermittelnde Ansicht Räume die Grundrechtsträger gegenüber der Öffentlichkeit nicht beherrscht oder zu deren Zutritt er nicht individuell die Erlaubnis erteilt, von Beginn an vom Wohnungsbegriff ausklammern. In der Tat erscheint es allerdings – auch unter dem Verweis auf die historische Rechtsprechung – den Wortlaut überzustrapazieren, wenn die weiteste Ansicht beispielsweise auch Supermärkte vom Schutzbereich umfasst wissen will. Ein aus Art. 13 GG folgender Kernbereichsschutz kann daher nur an solchen Orten (auch außerhalb der Wohnung im engen Sinne) bestehen, die der Grundrechtsträger unter seiner Herrschaft weiß und zu dem er die Eintretenden Personen individuell „einladen" kann.

bb) Beeinträchtigung

(1) Im Rahmen einer Wohnraumüberwachung nach § 100c StPO

Werden die Sensoren eines Sprachassistenten im Rahmen einer Wohnraumüberwachung nach § 100c StPO manipulativ zur Überwachung der in einem Wohnraum stattfindenden Gespräche aktiviert, stellt dies auch im Hinblick auf eine potentielle Grundrechtsbeeinträchtigung einen analog zum „großen Lauschangriff" zu beurteilenden Sachverhalt dar. Zwar handelt es sich beim hierzu notwendigen Aufspielen eines Abhörprogrammes über das Datennetz auf das Endgerät eines Sprachassistenten mangels physischer staatlicher Anwesenheit, noch nicht um eine Beeinträchtigung des Art. 13 GG. Dies ändert sich jedoch, wenn durch die Überwachung in der Wohnung ablaufende Vorgänge offenbart werden. Sodann werden aus den durch Art. 13 GG geschützten Wohnräumen Informationen gewonnen, die in diesem Bereich entstanden sind.[1138] Eine besondere Bedeutung kommt an dieser Stelle Art. 13 Abs. 3 GG zu, der dahingehend zu verstehen ist, dass er die Erhebung von Informationen im Rahmen der akustischen Wohnraumüberwachung erst dann nicht mehr rechtfertigen kann, wenn durch die Ermittlungsmaßnahme in den durch Art. 13 Abs. 1 i.V.m. Art. 1 Abs. 1 und Art. 2 Abs. 1 GG geschützten unantastbaren Bereich der

1138 *Schlegel*, GA 2007, 648, 656.

privaten Lebensgestaltung eingegriffen würde.[1139] Dies ist nach den oben aufgestellten Maßstäben zu beurteilen.

(2) Im Rahmen eines Zugriffs über § 100b StPO

Hinsichtlich der Aktivierung sensorischer Systeme des Sprachassistenten seitens der Strafverfolgungsbehörden wurde bereits ausgeführt, dass diese nicht auf Grundlage des § 100b StPO vorgenommen werden kann.[1140] Anders stellt sich die Situation dar, wenn ein infiltriertes Gerät durch den Nutzer selbst aktiviert wird und das Mikrofon sodann eine Informationsabfrage zur Weiterleitung an die Server des Sprachassistenten aufzeichnet. Insofern ist zu fragen, ob die heimliche Ausleitung eines solchen Sprachbefehls im Rahmen einer Live-Online-Überwachung ebenfalls ein Eingriff in den Schutzgehalt des Art. 13 GG darstellen würde. Zunächst ist diesbezüglich festzustellen, dass es an einem Eingriff in den Schutzbereich des Art. 13 GG nicht bereits deshalb fehlt, da die Wohnung der Zielperson zur Durchführung dieser Maßnahme nicht betreten werden muss. Denn Art. 13 GG soll nicht nur die räumliche Privatsphäre schützen, sondern dem Einzelnen ebenso einen Bereich innerhalb seiner eigenen vier Wände zusichern, in welchem dieser in Ruhe gelassen wird.[1141] Notwendig um einen Eingriff in Art. 13 GG in Erwägung zu ziehen ist allerdings, dass sich das informationstechnische System in einem vom Schutzbereich des Art. 13 Abs. 1 GG erfassten Raum befindet.[1142] Diese Voraussetzung erachtet das BVerfG bei der Durchsuchung von Datenträgern mittels einer Spionagesoftware als problematisch. Es begründet dies damit, dass ein solcher Zugriff unabhängig vom Standort des betroffenen Systems innerhalb einer Wohnung erfolgen könne.[1143] Insbesondere bei mobilen informationstechnischen Systemen wie Laptops, Personal Digital Assistants oder Mobiltelefonen sei der genaue Standort des infiltrierten Systems für die Ermittlungsmaßnahme ohne Bedeutung und darüber hinaus oftmals für die Behörden auch nicht erkennbar.[1144] Vergleicht man nun diesem mit dem der Live-

1139 BVerfGE 109, 279, 318.
1140 Vgl. § 4, B) V), 2), e).
1141 BVerfGE 51, 97, 107; 103, 142, 150; 115, 166, 196.
1142 *Kutscha*, NJW 2007, 1169, 1170 f.
1143 BVerfGE 120, 274, 310 f.
1144 BVerfGE 120, 274, 310 f.; *Gercke*, CR 2007, 245, 250, der ferner darauf hinweist, dass in diesen Fällen auch keine „räumliche Barriere" überwunden werden müsse.

Überwachung der Sprachassistentennutzung zugrunde liegende Sachverhalt, könnte daraus zu folgern sein, dass auch Sprachassistenten aufgrund ihrer Mobilität (sei es der mit dem Smartphone verbundene Sprachassistent Siri oder der mobile Sprachassistent Alexa) nicht vom Schutzbereich des Art. 13 GG umfasst seien. Dies ist für die Fälle, in welchen beispielsweise das komplette Smartphone des Betroffenen durchleuchtet werden soll, auch zutreffend. Sofern allerdings mittels einer Live-Online-Überwachung das Ziel verfolgt wird, die zwischen dem Betroffenen und seinem Sprachassistenten zukünftig ablaufenden Kommunikation zu erfassen, ist dieser, für die offline Durchsuchung des kompletten informationstechnischen Systems geltende Maßstab, nicht übertragbar. Im Unterschied zur offline Durchsuchung eines informationstechnischen Systems – für die der Standort des Systems tatsächlich ohne Belang ist – wird es zur Kommunikation mit dem Sprachassistenten grundsätzlich nur dann kommen, wenn der Betroffene sich an einem zurückgezogenen Ort aufhält, der in vielen Fällen dem weiten Wohnungsbegriff des Art. 13 GG entsprechen wird. Dies nicht bereits deswegen, da zum einen zu beobachten ist, dass sich viele Bürger in der Öffentlichkeit vor der Kommunikation mit einem Sprachassistenten scheuen und zum anderen die für die Strafverfolgungsbehörden bedeutenden Informationsabfragen selten dann besprochen werden, während der Betroffene sich an einem öffentlichen Ort befindet. Aufgrund dieser, zur klassischen offline Durchsuchung eines Datenträgers mit gespeicherten Inhalten, unterschiedlichen Situation, wird die Live-Überwachung der Sprachbefehle – solange sich der Betroffene in einer durch Art. 13 GG geschützten Räumlichkeit aufhält – eine Überwachung von Vorgängen innerhalb der Wohnung darstellen.[1145] Denn im Unterschied zur offline Online-Durchsuchung wird im Falle der Live-Online-Überwachung der private Rückzugsraum wie bei einer Durchsuchung oder einem Lauschangriff umfassend zur Informationserlangung genutzt.[1146] Eine Verwertbarkeit der auf diesem Wege erlangten Informationen wird sich daher auch an Art. 13 GG messen lassen müssen.

1145 Vgl. BVerfGE 120, 274, 310; *Rux*, JZ 2007, 285, 292; *Guttenberg*, NJW 1993, 567, 569; *Becker*, NVwZ 2015, 1335, 1136; *Huber*, NVwZ 2007, 880, 883; *Sachs/Krings*, JuS 2008, 481, 483.

1146 Vgl. *Schlegel*, GA 2007, 648, 659.

(3) Im Rahmen einer Maßnahme nach § 110 Abs. 3 StPO

Fraglich könnte der Schutz des Art. 13 GG sein, wenn die Strafverfolgungsbehörden in Kenntnis der Cloudzugangsdaten gem. § 110 Abs. 3 StPO eine Sicherungskopie der in der Cloud gespeicherten Audioaufzeichnungen anfertigen. Hierzu wird vertreten, dass es für die Gewährleistung des Grundrechtsschutzes keinen Unterschied mache, ob unmittelbar eine Durchsuchung der Wohnung[1147] und dabei auch eine Durchsicht der sich in dieser befindlichen informationstechnischen Systeme vorgenommen wird oder, ob über ein informationstechnisches System lediglich ein Zugriff auf ein externes Speichermedium erfolgt. Dieser Unterschied betreffe nur die Form der Datenübertragung und -speicherung, nicht die gespeicherten Daten selbst.[1148] Bei dieser Betrachtung kommt allerdings zu kurz, dass im Falle eines staatlichen Zugriffs, der die Verbindung des betroffenen Systems zu einem Rechnernetzwerk ausnutzt, die durch die räumliche Abgeschlossenheit der Wohnung vermittelte Privatsphäre unberührt bleibt.[1149] Der virtuelle Raum der Datenspeicherung ist faktisch kein Wohnraum i.S.d. Art. 13 GG.[1150] Auch hinsichtlich der übrigen sich in der Wohnung befindlichen Gegenstände ist anzumerken, dass deren Schutz durch das Wohnungsgrundrecht nicht darauf gründet, dass sich diese Gegenstände in einer Wohnung befinden, sondern diese lediglich reflexartig deshalb geschützt sind, da ein physischer Zugriff auf diese Gegenstände (Aktenordner, externe Festplatte) nur durch einen Eingriff in das Wohnungsgrundrecht ermöglicht werden kann. Bei virtuell gespeicherten Daten ist dies gerade nicht der Fall, da diese auch durch einen entsprechenden Fernzugriff erlangt werden können.[1151] Es fehlt dem Wohnungsgrundrecht folglich an einem Bezug zu elektronischen Beweismitteln, die auf einem externen Server gespeichert sind. Sofern es um die Sicherstellung, die Beschlagnahme oder die Durchsicht von solchen Daten geht, ist Art. 13 GG selbst dann nicht betroffen, wenn auf den virtuellen Datenraum mittels eines Gerätes innerhalb der Wohnung des Betroffenen zugegriffen wird oder sich das Zielgerät im Bereich einer Wohnung befin-

1147 Vgl. BVerfGE 103, 142, 150 f., wonach die physische Durchsuchung einer Wohnung mit einem erheblichen Eingriff in Art. 13 GG einhergeht.
1148 *Buermeyer*, HRRS 2007, 329, 333; *Rux*, JZ 2007, 285, 292 f.; *Schaar/Landwehr*, K&R 2007, 203, 204.
1149 Vgl. BVerfGE 120, 274, 310.
1150 *Brodowski/Eisenmenger*, ZD 2014, 119, 121.
1151 *Schlegel*, GA 2007, 648, 657.

det.[1152] Die Eingriffswirkung beschränkt sich vielmehr auf die Dauer eines womöglich eintretenden Sachentzugs und ist folglich an Art. 14 GG zu messen. Davon ausgehend, dass auf dem Sprachassistenten die gewünschten Audioaufzeichnungen ohnehin nicht gespeichert sind, wird ein solcher Sachentzug durch eine förmliche Beschlagnahme des Endgeräts vor Ort regelmäßig entbehrlich sein. Das Anfertigen einer bloßen Sicherungskopie der auf der Cloud vorgefundenen Audioaufzeichnungen stellt daher sowohl unter praktischen Gesichtspunkten als auch unter Verhältnismäßigkeitsgesichtspunkten das mildestes Mittel und damit die zu präferierende Vorgehensweise dar. Eine Beeinträchtigung der Eigentumsgarantie aus Art. 14 GG erfolgt sodann ebenfalls nicht.

b) Art. 10 GG

Dass die Nutzung eines Sprachassistenten sowohl während des Übertragungsweges als auch nach Speicherung der Nachrichten in der Cloud durch Art. 10 GG geschützt ist, wurde bereits dargelegt.[1153] Hingegen befinden sich die Audioaufzeichnungen vor dem Start eines Übertragungsvorganges ausschließlich auf dem Endgerät des Nutzers und damit noch in dessen alleiniger Herrschaftssphäre, sodass Art. 10 GG in diesem Stadium noch nicht einschlägig ist.

c) Computergrundrecht

Das Computergrundrecht stellt kein neues selbständiges Grundrecht dar, sondern wie das Recht auf informationelle Selbstbestimmung eine vom Bundesverfassungsgericht geschaffene konkretisierende Ausprägung des allgemeinen Persönlichkeitsrechts.[1154] Es gewährleistet die Vertraulichkeit und Integrität der informationstechnischen Systeme, die „*Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf dieses System es dem Staat [ermöglichen würde], einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar*

1152 BVerfG, NJW 2020, 384, Rn. 37; in die gleiche Richtung *Beulke/Meininghaus*, StV 2007, 63, 64; *Schlegel*, GA 2007, 648, 654 ff.
1153 Vgl. § 4, B), I), 2), b) cc); § 4, B), I), 2), c).
1154 *Dreier* in: Dreier-GG, Art. 2 Abs. 1 GG, Rn. 82.

ein aussagekräftiges Bild der Persönlichkeit zu erhalten".[1155] Im Lichte des IT-Grundrechts stellen sowohl das Endgerät des Benutzers vor Ort als auch der Sprachassistent in Form der Cloud des Dienstleistungsanbieters informationstechnische Systeme dar. Bei einer funktionalen Betrachtung verschmelzen das Endgerät sowie die durch den Dienstleistungsanbieter zu Verfügung gestellte Cloud zu einem einheitlichen informationstechnischen System im Sinne des IT-Grundrechts.[1156]

aa) Im Rahmen einer Wohnraumüberwachung nach § 100c StPO

Wie bereits dargestellt, kommt es bei der Infiltration eines Sprachassistenten zur Wohnraumüberwachung nach § 100c StPO mangels Berührungspunkten mit (bereits nicht vorhandenen) Daten auf dem Sprachassistenten zu keinem Eingriff in das IT-Grundrecht.[1157]

bb) Im Rahmen eines Zugriffs über § 100b StPO

Fraglich bleibt, ob in Fällen einer Live-Online-Überwachung nach § 100b StPO, in denen lediglich die durch den Sprachassistenten zur Weiterleitung an die Server aufgenommene Nachrichten, ausgeleitet werden, eine Beeinträchtigung des Computergrundrechts zu sehen ist. Im Unterschied zur Wohnraumüberwachung wird in einem solchen Fall der Sprachassistent nicht losgelöst von seiner eigentlichen Funktion als Wanze eingesetzt, sondern es werden konkret die Informationen ausgeleitet, die das informationstechnische System in seiner Funktion als Sprachassistent aufgezeichnet hat. Zwar lässt sich während eines Zugriffs auf den Übertragungsweg nur eine deutlich geringere Menge an Daten abgreifen als dies bei einer umfassenden Durchsuchung eines kompletten Datenträgers der Fall wäre. Der Umstand, dass sich so nur aktuelle Daten erheben lassen und hingegen solche, die in der Vergangenheit, vor Beginn der eingreifenden Maßnahme generiert worden unberücksichtigt bleiben, bedeutet nicht, dass ein Zugriff auf den Übertragungsweg zwischen Endgerät und Cloud keinen Eingriff in den Schutzbereich des IT-Grundrechts dar-

1155 BVerfGE 120, 274, 314.
1156 *Grözinger*, Die Überwachung von Cloud-Storage, S. 160.
1157 Vgl. oben § 4, B), VI).

stellen kann.[1158] Gestützt wird dies auch durch die Rechtsprechung des Bundesverfassungsgerichts, das betont, dass auch nur flüchtige Dateien dem Schutzbereich des IT-Grundrechts unterfallen.[1159] Ein Zugriff auf den Übertragungsweg zwischen dem durch den Nutzer benutzten Endgerät und der Sprachassistenzcloud erfüllt daher grundsätzlich die Voraussetzungen eines Eingriff in den Schutzbereich des IT-Grundrechts.

Insofern ist allerdings zu beachten, dass das Ausfiltern der an den Sprachassistenten gerichteten Sprachbefehle und der darauf erhaltenen Antworten eine Überwachung des Beschuldigten darstellt, die ebenso durch Art. 10 GG geschützt ist.[1160] Da der gleiche Sachverhalt sodann allerdings zwei unterschiedlichen grundrechtlichen Schutzbereichen unterfallen würde, ist deren Verhältnis zueinander zu klären. Der erste Senat ging in seiner Entscheidung zur Online-Durchsuchung von einem grundsätzlichen Vorrang des Telekommunikationsgeheimnisses aus, das den alleinigen grundrechtlichen Maßstab darstellt, sofern ein Vorgang laufender Fernmeldekommunikation vorliege.[1161] Dem schloss sich auch der zweite Senat an, der betont, dass der Schutz des IT-Grundrechts nur dann besteht, soweit andere Grundrechte, insbesondere Art. 10 GG, kein ausreichendes Schutzniveau gewährleisten können.[1162] In der BKAG-Entscheidung bestätigte das BVerfG schließlich nochmals seine aktuelle Rechtsprechung, dass ein Zugriff auf ein informationstechnisches System bei welchem durch rechtliche Vorgaben und technische Vorkehrungen sichergestellt ist, dass sich der Zugriff auf die Erfassung der laufenden Telekommunikation beschränkt, ausschließlich in das Telekommunikationsgeheimnis eingreift.[1163] Dagegen betont das Gericht in einer nur unwesentlich späteren Entscheidung, dass es sich bei Art. 10 GG im Vergleich zum IT-Grundrecht regelmäßig um die „speziellere Garantie" handelt.[1164] Damit distanzierte sich das Bundesverfassungsgericht von der bestehenden Ansicht, dass das IT-Grundrecht sowie Art. 10 GG in einem Exklusivitätsverhältnis

1158 So auch *Grözinger*, Die Überwachung von Cloud-Storage, S. 161.
1159 BVerfGE 120, 274, 324.
1160 Vgl. § 4, B), I), 2), b) cc); § 4 B), I), 2), c).
1161 BVerfGE 120, 274, 309; *Bantlin*, JuS 2019, 669, 670.
1162 BVerfGE 124, 43, 57.
1163 BVerfGE 141, 220, Rn. 228.
1164 BVerfG, Beschluss vom 06. Juli 2016 – 2 BvR 1454/13 -, Rn. 42 = teilweise in NJW 2016, 3508 ff.

stünden[1165] und bejahte die bloße Subsidiarität des IT-Grundrechts. Somit können zwar beide Schutzbereiche eröffnet sein, wobei das IT-Grundrecht allerdings durch das Telekommunikationsgeheimnis verdrängt wird und das staatliche Verhalten lediglich in den Schutzbereich des spezielleren Grundrechts einen zu rechtfertigenden Eingriff darstellt.

Wenn teilweise auch bei der Überwachung der Aktivitäten des Beschuldigten über das Internet eine Beeinträchtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme angenommen wird,[1166] so kann dies unterschiedliche Gründe haben. Zum einen kann ein divergierendes Schutzbereichsverständnis des Art. 10 GG[1167] zu der Situation führen, dass in der hier zugrunde liegenden Sachverhaltskonstellation bereits der Schutzbereich des Art. 10 GG nicht als eröffnet angesehen wird.

Zum anderen ist denkbar, dass außer Acht gelassen wird, dass der subsidiäre Schutz des IT-Grundrechts nur dann greift, wenn auf ein informationstechnisches System zugegriffen wird und dabei abgelegte Daten ohne Bezug zu einer telekommunikativen Nutzung des Systems erlangt werden.[1168] Kommt es wie bei der Live-Überwachung der Nutzung des Sprachassistenten zu einer Überwachung der hierüber ablaufenden Internetkommunikation, wird ohne Zugriff auf den Sprachassistenten nur die während des Übermittlungsvorgangs vom Benutzer an den Server sowie die anschließend vom Server an den Nutzer übertragenen Daten in Kopie an die Strafverfolgungsbehörden ausgeleitet.[1169] Die Situation stellt sich nicht derart dar, dass eine staatliche Stelle die Nutzung eines informationstechnischen Systems (daher die Erzeugung, Verarbeitung und Speicherung von Daten direkt auf dem informationstechnischen System)[1170] als solche überwacht oder die Speichermedien des Systems durchsucht. Nur dann würde es sich um die Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation handeln und das IT-Grundrecht wäre

1165 *Buermeyer*, StV 2013, 470, 475, der bei laufender Kommunikation eine Ausnahme vom Schutzbereich des IT-Grundrechts sieht und daher wohl von einem Exklusivitätsverhältnis ausgeht.

1166 LG Ellwangen, ZD 2014, 33, 36.

1167 *Grözinger*, Die Überwachung von Cloud-Storage, S. 171 f.; vgl. insofern die unterschiedlichen Ansichten zum Schutzbereich des Art. 10 GG, § 4, B), I), 2), b), cc).

1168 Zutreffend *Bär*, ZD 2014, 36, 38.

1169 Vgl. *Bär*, ZD 2014, 36, 38.

1170 BVerfGE 120, 274, 305.

anstelle des Art. 10 Abs. 1 GG einschlägig.[1171] Da dies bei der hier vorliegenden Fallkonstellation jedoch nicht der Fall ist, wäre nach der hier vertretenen Auffassung zum Schutzbereichsverständnis des Art. 10 GG der durch diesen gewährte Schutz vorranging.

cc) Im Rahmen einer Maßnahme nach § 110 Abs. 3 StPO

Anders könnte dies erneut im Rahmen eines Vorgehens der Ermittlungsbehörden gem. § 110 Abs. 3 StPO zu beurteilen sein. Bei der sodann erfolgten Datenerhebung aus der Cloud als komplexes informationstechnisches System besteht aufgrund der Vielzahl dort abgespeicherter Audioaufzeichnungen Potential für die Ausforschung der Persönlichkeit des Betroffenen.[1172] Allerdings soll das IT-Grundrecht bereits tatbestandlich nicht einschlägig sein, wenn eine staatliche Stelle aus einem informationstechnischen System die Daten auf einem technisch dafür vorgesehenen Weg erhebt.[1173] Auch wenn sich die Strafverfolgungsbehörden im Wege des Keyloggings in Kenntnis der Zugangsdaten versetzen, um auf den zugangsgeschützten Cloud-Speicher des Betroffenen Webseite zuzugreifen, würden die Behörden die Inhalte in Form der Audioaufzeichnungen auf dem dafür vorgesehenen Weg durch einen Login zur Cloud zur Kenntnis nehmen.[1174] Ferner wäre auch in diesem Fall der speziellere Schutz des Art. 10 GG zu beachten, der die infolge der Nutzung eines Sprachassistenten gespeicherten Nachrichten auch dann schützt, wenn die Nachrichten auf dem Server des Betreibers ruhen.[1175] Selbst bei einer tatbestandlichen Einschlägigkeit würde das IT-Grundrecht hinter der Garantie des Art. 10 GG zurücktreten.[1176]

d) Das Grundrecht auf informationelle Selbstbestimmung

Gewissermaßen als „Auffanggrundrecht" hinter den dargestellten speziellen Schutzbereichen steht das allgemeine Grundrecht auf informationel-

1171 Vgl. BVerfGE 120, 274, 308.
1172 Vgl. BVerfGE 120, 274, 322.
1173 BVerfGE 120, 274, 341.
1174 BVerfGE 120, 274, 341.
1175 Vgl. § 4, B), I), 2), c).
1176 vgl. zur subsidiären Schutzfunktion des IT-Grundrechts, BVerfGE 120, 274, 302; BVerfGE 124, 43, 57; *Gercke* in: HK-StPO, § 100b StPO, Rn. 2.

le Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Dieses schützt personenbezogene Daten vor staatlichem Zugriff jedweder Form unabhängig von einem bestimmten Kommunikations- oder Lebensbereich.[1177] In verschiedenen Ausgestaltungen beinhaltet es beispielsweise das Recht am eigenen Wort, dem eigenen Bild oder den Schutz der personalen Entfaltung.[1178] Von besonderer Relevanz ist im Zusammenspiel mit dem Zugriff auf Sprachassistenten freilich das Recht am gesprochenen Wort des Betroffenen. Der hierdurch verbürgte Schutz hat primär die Garantie einer ungestörten Teilnahme am zwischenmenschlichen Kommunikationsprozess zum Inhalt.[1179] Dadurch soll gewährleistet werden, dass der Grundrechtsträger im sozialen Leben unbefangen mit Dritten kommunizieren kann, ohne zu befürchten, dass seine vertraulichen, unbedachten oder spontanen Äußerungen aufgenommen und womöglich veröffentlicht oder gar in gerichtlichen Verfahren verwertet werden.[1180] Der Einzelnen soll stets das Verfügungsrecht über sein nicht öffentlich gesprochenes Wort in den Händen behalten, um selbst zu bestimmen, ob und wem seine privat gesprochenen Worte zugänglich sein sollen.[1181] Dies vermittelt dem allgemeinen Persönlichkeitsrecht eine Ergänzungsfunktion gegenüber Art. 10 und Art. 13 GG, die die kommunikative Persönlichkeitssphäre nur bei Vermittlung über bestimmte Informationsträger oder innerhalb geschützter Räumlichkeiten erfassen.[1182] Entsprechend kann das gesprochene Wort außerhalb des Gewährleistungsumfangs von Art. 13 Abs. 1 GG alleine über Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG einem umfassenden grundrechtlichen Schutz unterliegen. Entscheidend ist insofern, dass aus Sicht des Betroffenen nicht die Gefahr besteht, dass andere Personen außer der von ihm bedachten den Inhalt seiner Äußerungen erfassen können. Hält sich der Betroffene in seinem PKW für vollkommen alleine und abgeschnitten von der Außenwelt, ist die Nichtöffentlichkeit dieser Situation einer solchen in einer Wohnung gleichzusetzen, sodass auch die Aufzeichnung des gesprochenen Wortes an diesen Stellen eine rechtfertigungsbedürftige Grundrechtsverletzung des Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG darstellt.[1183] Der grundrechtliche Schutz des Betroffenen

1177 *Pieper*, JA 2018, 598, 602.
1178 *Epping*, Grundrechte, Rn. 631 ff.
1179 *Di Fabio* in: Maunz/Dürig-GG, Art. 2 Abs. 1 GG, Rn. 196.
1180 *Di Fabio* in: Maunz/Dürig-GG, Art. 2 Abs. 1 GG, Rn. 196; *Kleih*, Die strafprozessuale Überwachung der Telekommunikation, S. 54.
1181 BGH, NJW 1983, 1569, 1570; BVerfG, NJW 2020, 2699, Rn. 92.
1182 *Di Fabio* in: Maunz/Dürig-GG, Art. 2 Abs. 1 GG, Rn. 197.
1183 BGH, NJW 2012, 945, 946.

wird sich jedoch nur in solchen Fällen über Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG verwirklichen, in denen der Betroffene außerhalb des Art. 13 GG gem. § 100f StPO abgehört wird. Kommt es zum Ausleiten der Sprachbefehle während der aktiven Nutzung eines Sprachassistenten ist auch im Verhältnis zu Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG der speziellere Schutz des Art. 10 GG vorrangig.[1184]

2) Die Drei-Sphären-Theorie

Entscheidende Bedeutung im Rahmen der Verhältnismäßigkeitsprüfung zur Rechtfertigung eines Grundrechtseingriffes und damit auch der Entstehung eines selbstständigen Beweisverwertungsverbotes kommt der drei-Sphären Theorie zu. Die These, dass das Bundesverfassungsgericht im Volkszählungsurteil seine „Sphären-Rechtsprechung" aufgab,[1185] hat sich bei Betrachtung diverser Urteile der neueren Rechtsprechung nicht bestätigt.[1186] Die drei Sphären-Theorie unterscheidet zwischen Sozial-/ Privats- und Intimsphäre. Von der Betroffenheit der Sozialsphäre als „äußerste" dieser drei Sphären wird gemeinhin gesprochen, wenn der Einzelne im Rahmen des öffentlichen Lebens mit anderen Gesellschaftsmitgliedern interagiert.[1187] Hinsichtlich des durch diese Sphäre vermittelnden Grundrechtsschutzes ist festzuhalten, dass keine erhöhten Rechtfertigungsanforderungen zu stellen sind. Ein in einem formalen Gesetz zum Ausdruck kommendes öffentliches Interesse wird die Beschränkung des allgemeinen Persönlichkeitsrechts in diesem Bereich regelmäßig rechtfertigen.[1188] Im Unterschied hierzu reicht die Privatsphäre deutlich weiter in den Bereich der privaten autonomen Lebensgestaltung, in dem der Einzelne seine Individualität entwickeln und wahren kann. Damit werden typischerweise solche Handlungen erfasst, die öffentlich als unschicklich oder peinlich gelten und dadurch nachteilige Reaktionen der Mitmenschen auslösen würde.[1189] Auch wenn sich ein entsprechendes Verhalten regelmäßig in den häuslichen Rückzugsraum verlagern wird, ist der Schutzbereich der

---

1184 BVerfGE 100, 313, 358; *Martini* in: v. Münch/Kunig, Art. 10 GG, Rn. 232.
1185 *Desoi/Knierim*, DÖV 2011, 398, 401; *Hornung*, MMR 2004, 3.
1186 Vgl. zum Caroline-von-Monaco-Urteil, BVerfGE 101, 361; zum Fall Esra BVerfGE 119, 1; Auskunft nach Vaterschaftsanfechtung vgl. BVerfGE 138, 377.
1187 BVerfG, NJW 2003, 1109, 1100; BGH, NJW 1991, 1532, 1533; *Starck/Paulus* in: v. Mangoldt/Klein/Stark, Art. 5 GG, Rn. 331.
1188 *Starck/Paulus* in: v. Mangoldt/Klein/Stark, Art. 5 GG, Rn. 331.
1189 BVerfGE 101, 361, 382.

Privatsphäre nicht ortsgebunden, sondern erstreckt sich auf all diejenigen Örtlichkeiten und Situationen, in denen objektiv erkennbar davon ausgegangen werden darf, dass man der Öffentlichkeit nicht ausgesetzt ist.[1190] Entsprechend der sensibleren Inhalte, die der Privatsphäre zugeordnet werden, darf hier nur unter strikter Beachtung des Verhältnismäßigkeitsprinzips eingegriffen werden. Wobei allerdings zu beachten ist, dass aufgrund der Disponibilität der einzelnen Sphären der Schutz entfallen wird, wenn der Betroffene freiwillig private Angelegenheiten der Öffentlichkeit zugänglich macht.[1191] Der Übergang der Betroffenheit der Privatsphäre hin zur Betroffenheit der Intimsphäre gestaltet sich bisweilen fließend. Dass eine Zuordnung hierbei nicht zweifelsfrei erfolgen kann, zeigt bereits, dass das Bundesverfassungsgericht Auseinandersetzungen mit sich selbst in Tagebüchern, die vertrauliche Kommunikation unter Eheleuten, sozial abweichendes Verhalten, den Sexualbereich oder Krankheiten grundsätzlich der Privatsphäre zuordnet.[1192] Für andere wiederum ist die Betroffenheit der inneren Gedanken-/ und Gefühlswelt sowie des Sexualbereichs grundsätzlich so eng mit der Menschenwürde verbunden, dass solche Vorgänge unter die unabwägbare Intimsphäre fallen müssten.[1193] In einer neueren Entscheidung trennt schließlich das Bundesverfassungsgericht selbst nicht mehr zwischen Privat- und Intimsphäre, sondern verwendet die Begriffe scheinbar synonym.[1194] Zurecht wirft *Gless* die Frage

---

1190 BVerfGE 101, 361, 383 f.

1191 BVerfGE 101, 361, 384 f.

1192 Vgl. m.w.N. BVerfGE 101, 361, 382.

1193 *Starck/Paulus* in: v. Mangoldt/Klein/Stark, Art. 5 GG, Rn. 329.

1194 BVerfGE 138, 377, Rn. 29; *Dreier* in: Dreier-GG, Art. 2 GG, Rn. 71; Hinsichtlich der terminologischen Abgrenzung zwischen dem Kernbereich und der Intimsphäre sprach das Bundesverfassungsgericht gerade in seiner älteren Rechtsprechung kaum vom Schutz des Kernbereiches, sondern zog stets die Sphärentheorie heran. In den letzten Jahren ist zunehmend auch vom Schutz des Kernbereichs die Rede. In die gleiche Richtung geht eine Gesetzesbegründung aus dem Jahre 2004, die den Begriff des „Kernbereichs" gegenüber dem der Intimsphäre zu präferieren versucht, da dem Begriff der Intimsphäre eine nicht gewollte Enge anhafte, die den Begriff im natürlichen Sprachgebrauch auf die Bereiche Sexualität und Nacktheit reduziere, vgl. BS-Drs. 15/2466, S. 4. Hinzu kommt, dass der Begriff der Intimsphäre weniger mit einer im Kern strafprozessualen, als vielmehr mit einer rein grundrechtlichen bzw. verfassungsrechtlichen Fallgestaltung assoziiert wird. Nicht zuletzt durch die Kodifizierung des Begriffs „Kernbereich" in § 100d StPO wird dieser Begriff mit dem Strafprozessrecht in Verbindung gebracht. Letztlich führen sämtliche Versuche einer Abgrenzung jedoch nicht zu einem relevanten Mehrwert. Überhaupt gehen die Begrifflichkeiten der Intimsphären und des Kernbereichs

auf, ob die Drei-Sphären-Theorie als theoretisches Fundament für Beweisverbote auch in einer zunehmend digitalen Lebenswelt noch zeitgemäß ist.[1195] Und in der Tat ist es zutreffend, dass die Kernunterteilung im Rahmen dieser Theorie in sozial-privat-intim auch zukünftig in den Entscheidungen des BVerfG fortentwickelt werden muss, um Schritt mit den Veränderungen des tatsächlichen Lebens halten zu können.[1196] Zutreffend wurde in diesem Zusammenhang in der Entscheidung zur Online-Durchsuchung angedeutet, dass mit einer fortschreitenden elektronischen Erfassung Vernetzung der Daten die Unterscheidung zwischen sozial-privat-intim aufgrund Weiterentwicklung der Datenauslesbarkeit verwischt.[1197] Es ist dadurch auch möglich aus sozialen Daten Persönliches zu rekonstruieren (z.B. ein Bewegungs- oder Persönlichkeitsprofil des Betroffenen).[1198]

3) Zwischenergebnis

Bei der Prüfung der Grundrechtsbetroffenheit im Rahmen der staatlichen Überwachung der Nutzung eines Smart Speakers sowie des dahinterstehenden Sprachassistenten, ist hinsichtlich der heimlichen Ermittlungsmaßnahmen primär zwischen der Überwachung nach der Aktivierung des Sprachassistenten durch den Betroffenen sowie der unabhängig davon erfolgten Überwachung zu unterscheiden. Erfolgt eine Live-Überwachung nach § 100b StPO im Rahmen derer die aufgezeichneten Sprachbefehle mitgehört werden, handelt es sich dabei um einen an Art. 10 GG zu messenden Eingriff. Eine Aufzeichnung, die unabhängig von der Aktivie-

---

auf dasselbe Konzept, mit dem übergeordneten Ziel, das aus der Menschenwürde entspringende allgemeine Persönlichkeitsrecht zu schützen, zurück. Bereits dies macht eine finale Abgrenzung entbehrlich. Will man dennoch möglicherweise bestehenden begrifflichen Missverständnissen vorbeugen, so ist anzuregen, im Rahmen der strafprozessualen Beweiserhebung, die sich an den Normen der StPO orientiert, auf die drei-Sphären-Theorie zu verzichten und in Übereinstimmung mit § 100d StPO stets vom Schutz des Kernbereiches zu sprechen, der inhaltlich freilich Parallelen zur Intimsphäre aufweisen wird und aufweisen darf, vgl. auch *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, S. 32. Die Untergliederung in verschiedene Sphären sollte bei der verfassungsrechtlichen Abwägung (bspw. beim Entstehen eines selbstständigen Beweisverwertungsverbotes) verbleiben.

1195 *Gless*, StV 2018, 671, 677.

1196 *Gless*, StV 2018, 671, 677.

1197 *Gless*, StV 2018, 671, 677.

1198 *Hilgendorf/Valerius*, Internetstrafrecht, Rn 766.

rung des Sprachassistenten ablaufende Gespräche gem. § 100c StPO oder § 100f StPO überwacht, bleibt im Falle der Wohnraumüberwachung naturgemäß an den Voraussetzungen des Art. 13 GG zu messen. Erfolgt die Überwachung dagegen beispielsweise während einer Wanderung sind Art. 13 GG mangels örtlichen Bezugspunktes sowie Art. 10 GG mangels aktiv eingeleiteter Telekommunikation mit dem Sprachassistenten nicht einschlägig. Es tritt daher die subsidiäre Gewährleistung der informationellen Selbstbestimmung in den Vordergrund, die auch in dieser Situation das Recht am eigenen Wort grundrechtlich sichert. Bedacht werden muss, dass die staatliche Infiltration eines informationstechnischen Systems zur Überwachung nicht pauschal mit einem Eingriff in das IT-Grundrecht gleichgesetzt werden darf. Vielfach wird ein ausreichendes Schutzniveau durch die spezielleren Grundrechte in Form der Art. 13 GG und 10 GG gewährleistet sein. Selbst wenn diese – wie im Falle des Spaziergangs – nicht einschlägig sind, kann das Recht auf informationelle Selbstbestimmung, sofern es sich nicht um einem Zugriff auf gespeicherte ruhende Daten handelt, ein ausreichendes Schutzniveau für das gesprochene Wort bieten. Im Unterschied zum staatlichen Zugriff auf die Festplatten eines Computers, Smartphones und Notebooks oder zum Zugriff auf Cloud-Storage in Form einer Dropbox, kommt dem IT-Grundrecht bei der heimlichen Überwachung der Sprachassistenzüberwachung in Echtzeit eine untergeordnete Rolle zu. Schließlich liegt der Schwerpunkt während der Sprachassistentenüberwachung eindeutig in der Überwachung des „Jetzt" und nicht wie bei einem Zugriff auf einen physisch oder virtuelle Datenspeicher in der Vergangenheit.

Das IT-Grundrecht könnte lediglich dann Bedeutung erlangen, wenn im Rahmen eines umfassenden Zugriffs auf die in einer Cloud gespeicherten Audioaufzeichnungen – gleich ob im Wege einer Online-Durchsuchung des mit der Cloud verknüpften Computers oder einer offenen Durchsuchung mit anschließender Sichtung und Beschlagnahme beim Verdächtigen – auf sämtliche in der Cloud gespeicherten Audioaufzeichnungen zugegriffen würde. Sodann wird der Zugriff auf eine Sammlung ruhender Daten ermöglicht, die in ihrer Gesamtheit in der Lage sind, einen Einblick in die Lebensführung des Betroffenen zu gewähren. Die in der Cloud abgelegten Daten fallen folglich unbestritten unter den Schutzbereich des IT-Grundrechts.[1199] Allerdings ist damit nicht gesagt, dass das IT-Grundrecht das einzige Grundrecht zum Schutze der in einer Cloud gespeicherten Audioaufzeichnungen darstellt. Auch das BVerfG ging in

1199 BVerfGE 141, 220, 303, Rn. 209; *Gähler*, HRRS 2016, 340, 345.

seiner Entscheidung zur Online-Durchsuchung nur deshalb von einem notwendigen Schutz durch das IT-Grundrecht aus, da sich die abgegriffenen Daten lediglich auf einem heimischen Rechner befanden und die Ermittlungsmaßnahme dadurch nicht an Art. 10 Abs. 1 Var. 3 GG zu messen war, womit ansonsten eine Schutzlücke bestanden hätte.[1200] Folglich muss stets am konkreten Sachverhalt geprüft werden, ob auch bei einem Zugriff auf vermeintliche ruhende Daten nicht der vorrangige Schutz durch das Fernmeldegeheimnis einschlägig sein könnte. Insofern wurde bereits festgestellt, dass der durch Art. 10 GG gewährte Schutz auch nach der Speicherung der Audioaufzeichnungen in der Cloud fortbesteht.[1201] Es bleibt daher festzuhalten, dass der grundrechtliche Schutz der Nutzung eines Sprachassistenten, je nach den Gegebenheiten des Einzelfalls vollständig über die Art. 10 GG und Art. 13 GG sowie subsidiär über das Recht am eigenen Wort gewährleistet werden kann. Der grundrechtliche Schutz durch das IT-Grundrecht würde erst bei einer Schutzlücke, mithin soweit der Schutz nicht durch andere Grundrechte, wie Art. 10 GG, Art. 13 GG oder das Grundrecht auf informationelle Selbstbestimmung gewährleistet werden kann, greifen.[1202] Diese Schutzlücke wird regelmäßig erst erreicht sein, wenn Art. 10 GG mangels einer aktiv durchgeführten Telekommunikation, Art. 13 GG mangels dem fest zuzuordnenden Aufenthalt in einer hierdurch geschützten Räumlichkeit und das Recht auf informationelle Selbstbestimmung aufgrund eines Zugriffs auf einen ruhenden Datenbestand von erheblicher Bedeutung, keinen ausreichenden Schutz mehr gewährleisten kann.

4) Sonderkonstellation: Beweiserlangung durch Private

Von besonderer Brisanz in diesem Zusammenhang sind Situationen, in welchen die Beweismittel nicht primär durch einen Zugriff der Strafverfolgungsbehörden generiert werden, sondern diese sich lediglich die durch den Dienstleistungsanbieter erfolgten Aufzeichnungen zu Nutze machen. Denkbar sind hier die verschiedensten – im Folgenden zu beleuchtenden – Szenarien. Zu denken ist an den „klassischen" Fall, in dem die Strafverfolgungsbehörden auf den Dienstleistungsanbieter zugehen und bei diesem die Audioaufzeichnungen aus der Cloud des Beschuldigten beschlagnah-

1200 BVerfGE 120, 274, 307 f.
1201 Vgl. § 4, B), I), 2), c).
1202 BVerfGE 120, 274, 302.

men. Eine weitere Fallgestaltung läge darin, dass ein zur Verbesserung der Sprachassistenzsysteme angestellter Mitarbeiter des Dienstleistungsanbieters im Rahmen des Abhörens einer Audioaufzeichnung eine Straftat vermutet. Sodann stellt sich die Frage, ob diese Audioaufzeichnung, sofern sie vom Dienstleistungsanbieter den Strafverfolgungsbehörden unaufgefordert zur Verfügung gestellt wird, verwertbar ist. Daneben sind Situationen denkbar in denen der Sprachassistent, dass in der Wohnung gesprochene Wort ohne Wissen, mithin ohne Aktivierung durch die Nutzer aufgrund eines technischen Fehlers oder einer missverständlichen Aktivierung durch Raumgespräche oder Hintergrundgeräusche aufzeichnet.

a) Beschlagnahme aufgrund eines Anfangsverdachts

Unproblematisch gestaltet sich der Fall, in dem die Strafverfolgungsbehörden aufgrund eines Anfangsverdacht die in der Cloud gespeicherten Aufzeichnungen beim Betroffenen oder direkt beim Dienstleistungsanbieter beschlagnahmen. Sofern die Daten in der Cloud aufgrund einer aktiven Nutzung durch den Betroffenen gespeichert wurden entstehen keine weitergehenden Problematiken. Hinsichtlich des besonderen Inhalts der Audioaufzeichnungen, insbesondere sofern es sich dabei um Selbst- oder auch Zwiegespräche handelt, kann auf die obigen Ausführungen verwiesen werden. Eine Besonderheit stellt es hier einzig dar, dass das Beweisverwertungsverbot seine Grundlage sodann nicht in § 100d Abs. 2 StPO findet, da sich dieser lediglich auf Informationen bezieht, die durch Maßnahmen nach den § 100a StPO bis 100c StPO erlangt wurden. Stattdessen wird das den Kernbereich schützende Beweisverwertungsverbot in diesen Fällen unmittelbar aus den die Nutzung eines Sprachassistenten schützenden Grundrechte mithin der Verfassung abgeleitet (selbstständiges Beweisverwertungsverbot). An seiner Absolutheit vermag dies freilich nichts zu ändern.

b) Übermittlung einer autorisierten Aufzeichnung durch Dienstleistungsanbieter an die Strafverfolgungsbehörden

Problematischer stellt sich der Sachverhalt dar, wenn die Strafverfolgungsbehörden noch keinen Verdacht hinsichtlich einer bestimmten Person hatten und sodann ein mithörender Arbeitnehmer des Dienstleistungsanbieters diese Aufzeichnung der Polizei übermittelt. Die Beweisgewinnung

folglich nicht durch die Strafverfolgungsbehörden, sondern durch private (Wirtschaftsunternehmen) erfolgte. Wie eine solche „Beweisgewinnung durch Private" zu behandeln ist, ist seit Jahren streitig und erreichte im Jahre 2008 im Zuge der Lichtensteiner Steueraffäre ihren wohl vorzeitigen Höhepunkt.[1203] In der Regel findet sich zu diesem Themenfeld in Rechtsprechung und Literatur der floskelartige Hinweis, dass sich die Normen der StPO nur an die staatlichen Strafverfolgungsorgane, nicht aber an Privatpersonen richten.[1204] Hieraus wird sodann gefolgert, dass rechtswidrig durch Private beschaffene Beweismittel verwertbar seien.[1205] Von diesem Grundsatz weicht die herrschende Meinung in drei Konstellationen ab: Erstens wenn die Erlangung des Beweismittels in krasser oder extremer Weise menschenrechtswidrig erfolgte, zweitens bei einem Eingriff in die Intimsphäre und drittens sofern der Staat durch die gezielte Beauftragung Privater Vorschriften der StPO umgehen wollte.[1206] Dieser Rechtsprechung wird durch Teile der Literatur entgegengehalten, sie verkenne durch ihr Abstellen auf den bloßen Adressatenkreis der StPO den eigentlich relevanten Anknüpfungspunkt der Entstehung eines selbstständigen Beweisverwertungsverbotes. Das für den Beschuldigten nachteilige, liege aus Sicht des im Zentrum stehenden Strafverfahrens weniger in der rechtswidrigen Beweisgewinnung, als vielmehr in dem den Beschuldigten eigentlich belastenden Akt der Verwertung, der wiederum unstreitig einen solchen hoheitlicher Natur darstelle.[1207] Diese Thematik würde im skizier-

---

1203 Vgl. dazu im Detail ausführlich *Trüg/Habetha*, NStZ 2008, 481; *dies*. NJW 2008, 887.

1204 BGHSt 27, 355, 357; BGHSt 36, 167, 173; *Bader* in: KK-*StPO,* Vor. § 48 StPO, Rn. 52; *Diemer* in: KK-StPO, § 136a StPO, Rn 3; *Schmitt* in: Meyer-Goßner/Schmitt, § 136a StPO, Rn. 3; *Schneider*, NStZ 2001, 8, 12.

1205 BGHSt 27, 355, 357; BGHSt 36, 167, 173; *Schmitt* in: Meyer-Goßner/Schmitt, § 136a StPO, Rn. 3; *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 65; *Beulke/Swoboda*, Strafprozessrecht, Rn. 730; FS-Kleinknecht/*Otto*, 319, 338; FS-Spendel/*Ranft*, S. 719, 736; *Kaspar*, GA 2013, 206, 207.

1206 *Bader* in: KK-StPO, vor § 48 StPO, Rn. 52; *Wolter* in: SK-StPO, § 136a StPO, Rn 15; *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 65; *Beulke/Swobdoda*, Strafprozessrecht, Rn. 730 ff.; *Kindhäuser*, StPO, § 23, Rn. 34 ff.; *Schmitt* in: Meyer-Goßner/Schmitt, § 136a StPO, Rn 3; vgl. zu möglichen Fällen der staatlichen Veranlassung auch *Stoffer*, Privatisierung des strafprozessualen Ermittlungsverfahren, S. 321 ff.; für eine ausführliche Darstellung der Thematik vgl. *Zeyher*, Strafprozessuale Beweisverwertung von privatem Videomaterial, S. 110 ff.

1207 *Trüg*, Lösungskonvergenzen trotz Systemdivergenzen, S. 311 f.; *Gropp*, StV 1989, 216, 220; *Dencker*, Verwertungsverbote im Strafprozess, S. 109; *Brunhöber*, GA 2010, 571, 587; *Dalakouras*, Beweisverbote und Intimsphäre, S. 272.

ten Fall allerdings nur dann von tragender Relevanz, wenn in der Art der Beweisgewinnung durch den Dienstleistungsanbieter ein rechtswidriger Akt zu sehen wäre. Der hierauf zu untersuchende Vorgang liegt in der auditiven und verschriftlichten Speicherung der Audioaufzeichnung in der eigenen Cloud. Sofern dieses Verhalten gar strafrechtlich relevant wäre, würde es sich in jedem Fall um eine rechtswidrige Beweisgewinnung durch Private handeln.

aa) § 201 Abs. 1 Nr. 1 StGB

Relevant wird hier § 201 Abs. 1 Nr. 1 StGB, der als Rechtsgut das gesprochene Wort schützt. Tatbestandlich erfordert § 201 StGB die Unbefugtheit der Aufzeichnung. Ohne weitergehende Auseinandersetzung mit diesem Tatbestandsmerkmal wird in der herkömmlichen Konstellation der bewussten Nutzung eines Sprachassistenten jedoch ein konkludentes Einverständnis mit der Speicherung der Aufzeichnungen in der Cloud zu sehen sein. Amazon weist seine Kunden beispielweise in den Nutzungsbedingungen ihrer Sprachassistenten drauf hin, dass zur Verarbeitung der Sprachbefehle eine Weiterleitung und Speicherung der Audioaufzeichnungen in der Cloud erfolgt.[1208] Wenn der Nutzer sodann trotz dieser Kenntnis in einen Informationsaustausch tritt, obwohl er dies ohne Konsequenzen auch unterlassen könnte, ist darin ein konkludentes Einverständnis zu sehen.[1209] Strafrechtlich ist in der Aufzeichnung des gesprochenen Wortes im Falle der bewussten Aktivierung aufgrund eines tatbestandsausschließenden Einverständnisses daher keine unbefugte Aufzeichnung zu sehen.[1210] Mangels eines rechtswidrigen Beweisgewinnungsakts kommt der Thematik der rechtswidrigen Beweisgewinnung durch Private (hier durch Unternehmensangestellte) in diesem Fall keine Bedeutung zu.

1208 Vgl. https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (zuletzt abgerufen am 31.10.2021).

1209 Vgl. *Kühl* in: Lackner/Kühl, § 201 StGB, Rn. 11.

1210 Vgl. *Eisele* in: Schönke/Schröder, § 201 StGB, Rn. 13; *Graf* in: MüKo-StGB, § 201 StGB, Rn. 22; *Schünemann* in: LK-StGB, § 201 StGB, Rn. 9; andere gehen dagegen von einer rechtfertigenden Einwilligung aus *Fischer*-StGB, § 201, Rn. 10.

bb) § 206 StGB

Daneben könnte die Weitergabe der im Rahmen einer Anfrage an den Sprachassistenten aufgezeichneten Audiodateien durch Mitarbeiter der Dienstleistungsanbieter den Straftatbestand des § 206 Abs. 1 StGB erfüllen. Danach wird bestraft wer, unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt. Gem. § 206 Abs. 5 S. 2 StGB unterfällt dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände. Die entsprechenden Audioaufzeichnungen eines Sprachassistenten stellen damit ein taugliches Tatobjekt dar.[1211] Von der Strafnorm werden jedoch ausschließlich Unternehmen erfasst, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen. Dies liegt darin begründet, dass der Schutzzweck des § 206 StGB nicht der Schutz vor Indiskretion seitens des Kommunikationspartners (hier des Telemedienanbieters) ist, sondern der Schutz vor besonderen Gefahren im Rahmen der Übermittlung einer Nachricht.[1212] Auch wenn die Daten durch die alleinige Speicherung im Herrschaftsbereich des Telemediendienstleisters fortlaufend von Art. 10 GG gegen fremden Zugriff geschützt sind, liegt die Situation in dem Fall, in dem der Telemediendienstleistungsanbieter Nutzer- oder Inhaltsdaten bewusst an die Strafverfolgungsbehörden weitergibt so, dass dadurch lediglich das in den Telemedienanbieter gesetzte Vertrauen in einen ordnungsgemäßen Umgang mit den ihm übertragenen Inhaltsdaten enttäuscht wird.[1213] Bei den Anbietern von Cloud Dienstleistungen zur Nutzung eines Sprachassistenten handelt es sich wie gesehen um Telemediendienstleister, die gem. § 1 TMG gerade nicht als Telekommunikationsdienstleister eingestuft werden können.[1214] Eine Strafbarkeit der Mitarbeiter eines solchen Unternehmens scheidet im Fall der Übergabe entsprechender Informationen an die Strafverfolgungsbehörden ohne amtlich Anordnung de lege lata aus.

1211 Vgl. auch oben § 4, B., I), 2), b), cc).
1212 *Eisele* in: Schönke/Schröder, § 206 StGB, Rn. 6b; *Heger* in: Lackner/Kühl, § 206 StGB, Rn. 13; *Kargl*, in: NK-StGB, § 206 StGB, Rn. 17.
1213 *Müller*, Cloud Computing, S. 198.
1214 *Altenhain* in: MüKo-StGB, § 206 StGB, Rn. 21; vgl. oben § 4, B., IX), 2), b), cc), (2).

c) Übermittlung einer nicht autorisierten Aufzeichnung an die Strafverfolgungsbehörden

Weit diffiziler stellt sich dies jedoch dar, wenn die Sprachaufzeichnung und damit die Speicherung der Audioaufzeichnungen in der Cloud ohne die bewusste Aktivierung des Sprachassistenten erfolgt. Dabei sind verschiedene Konstellationen denkbar. So ist denkbar, dass sich der Sprachassistent Alexa bei dem Rufen einer ähnlich heißenden Person (bspw. Alexander oder Alexandra) oder durch Wahrnehmung der übrigen Aktivierungsworte „Computer" und „Echo" – beispielsweise durch Hintergrundgeräusche – aktiviert. In diesen Fällen fehlt es folglich an einer bewussten Aktivierung des Sprachassistenten durch den Betroffenen. Es ist zu fragen, ob dies auch etwas an der strafrechtlichen Wertung i.S.d. § 201 Abs. 1 Nr. 1 StGB zu ändern vermag.

aa) § 201 Abs. 1 Nr. 1 StGB

Tatbestandlich wird das gesprochene Wort unabhängig von der Art und Weise der Äußerung geschützt, solange es sich um eine unmittelbare, akustisch wahrnehmbare Äußerung von Gedankeninhalten mittels lautbarer Zeichen handelt.[1215] Unter das gesprochene Wort fallen in diesem Sinne nicht nur das bewusst Gesprochene, sondern auch unbewusste Äußerungen im Rahmen eines Selbstgespräches.[1216] Nichtöffentlich sind die Äußerungen, wenn sie nicht für einen größeren, nach Zahl und Individualität unbestimmten oder nicht durch persönliche Beziehungen miteinander verbundenen Personenkreis bestimmt oder durch diesen unmittelbar wahrnehmbar sind.[1217] Dabei ist das gesprochene Wort auf einem Tonträger aufgenommen, wenn eine akustische Wiedergabe möglich ist.[1218]

Insoweit wäre die Nutzung eines Sprachassistenten – wie auch im obigen Beispiel – unter der Norm subsumierbar. Die Nutzung des Sprachassistenten an einem zurückgezogenen Ort erschafft eine Audiodatei, deren akustische Widergabe unproblematisch durch ein einfaches Abspielen

1215 *Fischer*-StGB, § 201 StGB, Rn. 3.
1216 *Heuchemer* in: BeckOK-StGB, § 201 StGB, Rn. 3.
1217 OLG Frankfurt a. M., NJW 1977, 1547; *Schünemann* in: LK-StGB, § 201 StGB, Rn. 8; *Heuchemer* in: BeckOK-StGB, § 201 StGB, Rn. 4.
1218 *Eisele* in: Schönke/Schröder, § 201 StGB, Rn. 11; *Joecks*-Studienkommentar, § 201 StGB, Rn. 5; *Kargl* in: NK-StGB, § 201 StGB, Rn. 10.

möglich ist. Entscheidend ist aber, ob die Aufzeichnung auch in diesem Fallbeispiel unbefugt erfolgt. Auf den in der Literatur herrschenden Streit zur dogmatischen Einordnung dieses Merkmals, soll hier, ob der vorliegenden Ergebnisgleichheit, nicht näher eingegangen werden: Zum einen könnte man dem Merkmal „unbefugt" eine doppelfunktionelle Funktion einerseits zur Einschränkung des Tatbestands bei Aufnahmen mit Einverständnis und andererseits zur Bezeichnung des allgemeinen Deliktsmerkmals der Rechtswidrigkeit zuweisen.[1219] Dem folgend könnte gegen ein die Unbefugtheit ausschließendes Einverständnis eingewandt werden, dass der Betroffene, sofern er sich einen smarten Assistenten kauft, mit dem Risiko einer unautorisierten Aufzeichnung rechnen muss. Insbesondere deshalb, da dieses Risiko auch in den Nutzungsbedingungen des Sprachassistenten Alexa explizit erwähnt wird.[1220] Eine solche Betrachtungsweise würde aber auf ein automatisches Abbedingen des Rechts auf informationelle Selbstbestimmung allein durch den Besitz eines Sprachassistenten hinauslaufen. Die Unbefugtheit kann damit erst bei einem Einverständnis im Sinne eines tatsächlich zustimmenden Willens des Sprechenden aufgehoben sein.[1221] Ein solcher zustimmender Wille kann lediglich dann angenommen werden, wenn der Betroffene die Speicherung zur Bearbeitung seines Sprachbefehls als notwendigen Zwischenschritt in Kauf nimmt. Da der Betroffene in den beschriebenen Situationen allerdings nicht einmal Kenntnis von der gerade stattfindenden Aufnahme haben wird, kann ein solcher Wille bereits nicht vorliegen. Vielmehr ähnelt die Situation der einer heimlichen Tonbandaufnahme. Heimlich auch deswegen, da der Betroffene mangels Kenntnis der Aufnahme, auch keine Veranlassung sehen wird, bestimmte Audiodateien wieder aus der Cloud löschen zu wollen. Die nicht durch bewusste Aufforderung autorisierte Aufzeichnung seitens eines Smart-Home Geräts stellt damit diesen Literaturströmen folgend mangels Einverständnisses eine unbefugte Handlung i.S.d. § 201 StGB dar.

Zum anderen könnte man das Merkmal dagegen rechtfertigungstechnisch verstehen, sodass unbefugt handelt, wer ohne Rechtfertigungsgrund die Tathandlung begeht.[1222] Auch bei dieser Sichtweise ergibt sich jedoch kein anderes Ergebnis. Sämtliche denkbaren Rechtfertigungsgründe schei-

1219 Vgl. *Eisele* in: Schönke/Schröder, § 201 StGB, Rn. 13.

1220 Vgl. https://www.amazon.de/gp/help/customer/display.html?nodeId=201602230 (zuletzt abgerufen am 31.10.2021).

1221 *Eisele* in: Schönke/Schröder, § 201 StGB, Rn. 13; *Kargl* in: NK-StGB, § 201 StGB, Rn. 23; *Kühl* in: Lackner/Kühl, § 201 StGB, Rn. 11; *Wessels/Hettinger/Engländer*, Strafrecht BT I, Rn. 494; Baumann-FS/*Lenckner*, 135, 147 f.

1222 *Fischer*-StGB, § 201 StGB, Rn. 9; *Hoyer* in: SK-StGB, § 201 StGB, Rn. 34.

den in jedem Fall aus, da die Aufzeichnung durch den Dienstleistungsanbieter ohne subjektives Rechtfertigungselement erfolgt. Diesem war im entscheidenden Zeitpunkt der unautorisierten Aufnahme nicht bewusst, dass diese Aufzeichnung strafrechtlich relevante Inhalte zum Gegenstand haben könnte. Auch an eine rechtfertigende Einwilligung, die diese Ansicht im Falle der aktiven Nutzung des Sprachassistenten annehmen würde, ist in dieser Fallkonstellation nicht zu denken.

Gleichwohl wird in diesen Fällen keine Strafbarkeit der verantwortlichen Angestellten des Dienstleistungsanbieters vorliegen. Die Aufzeichnung wird regelmäßig nicht auf deren vorsätzliches Verhalten, sondern schlicht auf eine technisch (noch) nicht ausschließbare Fehlinterpretation seitens des technischen Endgeräts zurückzuführen sein. Dabei würde es auch zu weit gehen, diesen Personen einen Eventualvorsatz dahingehend zu unterstellen, solche nicht gewollten Aufzeichnungen billigend in Kauf nehmen. Daher ist zwar keine Strafbarkeit gegeben, gleichwohl indiziert die Vollendung des objektiven Tatbestands, dass die so erlangten Aufzeichnungen nicht im Einklang mit der Rechtsordnung entstanden sind.

bb) Voraussetzungen und Folgen einer rechtswidrigen Beweisgewinnung durch Private

Daher ist zu fragen, wann von einer rechtswidrigen Beweisgewinnung mit den skizzierten Folgeproblemen auszugehen ist. Bedarf es hierfür eines aktiven Beweisbesorgungsvorgangs durch Privatpersonen oder genügt es bereits, wenn die Beweise durch Privatpersonen beiläufig beschafft werden? Daran anknüpfend stellt sich die Frage, ob eine rechtswidrige Beweisgewinnung zwangsläufig mit einer strafbaren Beweisgewinnung einhergehen muss.

Bei einem Blick auf die hierzu bisher ergangene Rechtsprechung, die größtenteils zweckgerichtete Beweisbeschaffungsakte zu bewerten hatte,[1223] könnte man anzunehmen, dass ohne eine solche Zweckgerichtetheit bereits keine zu problematisierende rechtswidrige Beweisgewinnung durch Private vorläge. Dass die durch Privatpersonen generierten Beweise

1223 BVerfG, NStZ 2011, 103 (Zusammenstellung von Steuerdaten CDs); BGHSt 31, 304 (Aufzeichnung eines Gesprächs durch V-Mann); BGHSt 34, 362 (Ausfragen des Beschuldigten durch Mitgefangenen); BGHSt 52, 11 (Drängen eines verdeckten Ermittlers auf Aussage); BGH NStZ 2011, 596 (private Tonaufnahme durch Informantin; LG Düsseldorf, NStZ-RR 2011, 84 (Datendiebstahl).

aber auch bei fehlender Zweckgerichtetheit zum Ziel der Beweisgewinnung nicht losgelöst von der hier genannten Problematik verwertet werden können, zeigt eine Entscheidung, in welcher die von einer mit dem Angeklagten befreundeten Zeugin gefertigten Handy-Aufzeichnung der Tat gegen den Angeklagten verwertet werden sollte und im Zusammenhang hiermit ebenfalls die rechtswidrige Beweisgewinnung durch Privatpersonen thematisiert wurde.[1224] Dessen Freundin hatte die Videoaufzeichnung selbstredend nicht zum Zwecke der Beweisgewinnung für ein späteres Strafverfahren gegen ihren Bekannten angefertigt. Es ist daher für die Diskussion über eine möglicherweise die Verwertbarkeit ausschließende Beweisgewinnung durch Private nicht erforderlich, dass der Private (hier die handelnden Personen hinter dem Dienstleistungsanbieter) die Beweise zielgerichtet zum Zwecke der Strafverfolgung generieren wollte.

Ferner ergibt sich aus Rechtsprechung auch nicht, dass eine rechtswidrige Beweisgewinnung gleichbedeutend mit einer materiellen Strafbarkeit sein muss. Vielmehr bedeutet rechtswidrig einen generellen Verstoß gegen gesetzliche Vorschriften.[1225] Entscheidend ist an dieser Stelle, dass die verletzte Norm gerade dem Grundrechtsschutz des Betroffenen dient.[1226] Eine Aufzeichnung des gesprochenen Wortes ohne Autorisierung durch den Nutzer verletzt diesen daher grundsätzlich in seinem informationellen Selbstbestimmungsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.[1227] Diese Verletzung würde sich an anderer Stelle auch in einem zivilrechtlichen Unterlassungs- und Löschungsanspruch analog § 823 Abs. 1 BGB i.V.m. § 1004 Abs. 1 S. 1 BGB widerspiegeln. Bekanntermaßen garantiert das aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG folgende allgemeine Persönlichkeitsrecht dem Einzelne grundsätzlich die alleinige Verfügungsgewalt, wer Besitz von den sein gesprochenes Wort manifestierenden Audioaufzeichnungen erlangen darf. Die Eigenschaft des allgemeinen Persönlichkeitsrechts als Rahmenrecht bringt zwar mit sich, dass nicht jede Beeinträchtigung eines solchen Rahmenrechte die Rechtswidrigkeit der Handlung indiziert, sondern diese von einer Güter- und Interessenabwägung im Einzelfall abhängig ist.[1228] Im Falle der unautorisierten Aufzeichnung, nicht für die Verarbeitung durch den Sprachassistenten bestimm-

1224 BGH, JR 2016, 542, 542.
1225 Vgl. *Niehaus*, NZV 2016, 551, 552.
1226 *Niehaus*, NZV 2016, 551, 552 f.; *Bachmeier*, DAR 2014, 15, 20.
1227 BVerfGE 34, 238, 246.
1228 *Klass* in: Erman-BGB, Anhang zu § 12, Rn. 11; *Slizyk* in: Slyzik, Handbuch Schmerzensgeld, Rn. 174.

ter Gespräche, sind jedoch – insbesondere, wenn diese Aufzeichnung in einem privaten Rückzugsort erfolgt – keine Gründe ersichtlich, wieso die Rechtswidrigkeit solcher Aufzeichnungen entfallen sollte. Die auf diesem Wege generierten Beweismittel stehen folglich in einem Widerspruch zu gesetzlichen Vorschriften und sind damit auch rechtswidrig erlangt. Der Umstand, dass mangels Vorsatzes keine Strafbarkeit vorliegt, kann im Rahmen der von der Rechtsprechung zur Ermittlung eines selbstständigen Beweisverwertungsverbotes herangezogen Abwägung maximal „verwertungsfördernd" berücksichtigt werden, vermag aber an der rechtswidrigen Beweiserlangung nichts zu ändern.

(1) Lösung der Rechtsprechung und Teilen der Literatur

Von einem rechtswidrig gewonnenen Beweismittel ausgehend, würde die Rechtsprechung und sich ihr anschließend Teile der Literatur, sofern keine der ohnehin für ein Verwertungsverbot sprechenden Ausnahmen erfüllt sind, im Rahmen einer Abwägung entscheiden, ob ein Beweisverwertungsverbot angenommen wird.[1229] Für eine menschenrechtswidrige Beweisgewinnung fehlt es im hiesigen Beispiel an der erforderlichen Rechtsverletzungsqualität, weil die – zudem unbeabsichtigte Aufzeichnung von Gesprächen – in keiner Weise an die eklatanten Extremübergriffe wie Folter heranreichen kann. Ferner wurde die Aufzeichnung nicht staatlich veranlasst oder ein Privater gezielt mit der Beweisbeschaffung beauftragt, um die im Falle eines eigenen staatlichen Tätigwerdens bestehenden grundrechtlichen Verpflichtungen zu umgehen. Hieran könnte allenfalls zu denken sein, wenn der Dienstleistungsanbieter wiederholt oder dauerhaft eigenmächtig mittels nicht durch den Nutzer in Gang gesetzten Aufzeichnungen Beweismittel für staatliche Stellen generieren möchte und sich so zu einem selbsternannten „Hilfssheriff" aufschwänge und dies durch die Behörden hingenommen würde.[1230] Die Rechtsprechung würde daher in der Regel nur über den Weg, dass die Verwertung des Materials einen

1229 Vgl. BGHSt 36, 167, 174; BGH, Beschluss vom 18.08.2020 – 5 StR 175/20; BGH, Beschluss vom 18.08.2021 – 5 StR 217/21; BVerfGE 34, 238, 242; auch der EGMR sieht in der Verwertbarkeit eines rechtswidrig durch eine Privatperson aufgezeichneten Gespräch kein Verstoß gegen den Grundsatz auf ein faires Verfahren, sofern die Rechte der Verteidigung gewahrt wurden und die Verurteilung nicht ausschließlich auf dem rechtswidrig erlangten Beweismittel beruht, vgl. EGMR, NJW 1989, 654, 656; *Kohlhaas*, DRiZ 1966, 286, 289.

1230 OLG Stuttgart, NJW 2016, 2280, 2282.

eigenen und ungerechtfertigten, da die Intimsphäre betreffenden, Grundrechtseingriff darstellt, zu einem Beweisverwertungsverbot gelangen. Von einer Betroffenheit der Intimsphäre würde die Rechtsprechung jedoch erneut nur bei einem Selbstgespräch ausgehen.[1231] Gleichwohl entschied das Bundesverfassungsgericht, dass der mit der Verwertung einhergehende Eingriff in das Persönlichkeitsrecht beim Abspielen von rechtswidrig durch eine Privatperson aufgenommenen Tonbandaufnahmen, die einen Betrug und eine Steuerhinterziehung beweisen sollten, nicht im Rahmen der Verhältnismäßigkeit gerechtfertigt werden kann.[1232] Dennoch – und dies betont das Gericht selbst, kann in anderen Fällen eine Abwägung unter Heranziehung des Strafverfolgungsinteresses in Form der Tatschwere und dem Umstand einer womöglich materiell nicht strafbewährten Beweisgewinnung zu einer Verwertbarkeit der auf diesem Wege erlangten Informationen führen.[1233]

(2) Literaturstimmen

Kritisch zu beachten sei diese Rechtsprechung, da die einzige Schranke, die sie einer Verwertbarkeit rechtswidrig erlangter Informationen durch Private gegenüberstellt in den drei genannten Fallgruppen zu sehen ist. Tatsächlich stellen die Fälle der Menschenrechtsverletzung, Intimsphärenverletzung oder die bewusste Umgehung der Beweiserhebungsvorschriften durch die Einschaltung Privater krasse Ausnahmefälle dar. In einem Großteil der durch Private erlangten Beweismittel würde die damit möglicherweise einhergehende Rechtswidrigkeit aber schlicht übergangen. Daher wird teilweise gefordert, dass ein Beweisverwertungsverbot bei einer rechtswidrigen Beweisgewinnung durch Private dann vorliege, wenn dies auch nach der bei einer staatlichen Beweisgewinnung geltenden Rechtslage der Fall gewesen wäre.[1234] Wäre die Aufzeichnung entsprechend durch die staatlichen Strafverfolgungsbehörden erfolgt, stünde hierfür zwar eine hypothetische Ermächtigungsgrundlage in Form des § 100b StPO und § 100c StPO zur Verfügung, allerdings hatten die Behörden gerade keinen entsprechenden Anfangsverdacht, sodass eine entsprechende Beweiserhe-

1231 Vgl. § 5, A., I), 1), d), bb), (3).
1232 BVerfGE 34, 238, 249 ff.; vgl. auch FS-Jescheck/*Herrmann*, 1291, 1305; *Jescheck*, 46. DJT, Bd. I, 1, 48.
1233 BVerfGE 34, 238, 249 ff.
1234 *Niehaus*, NZV 2016, 551, 552; *Rogall*, ZStW 1979, 1, 42.

bung durch den Staat auf keine einschlägige Ermächtigungsgrundlage hätte gestützt werden können. Selbst wenn man mit der Rechtsprechung die Annahme eines Beweisverwertungsverbots auf der Basis von „Abwägungen" bestimmen würde, wäre in dem Fall einer solchen anlasslosen, da ohne Anfangsverdacht, durchgeführten Überwachung ein Fall des willkürlichen Eingriffs in Grundrechte zu erblicken und die Annahme eines Verwertungsverbotes zwingend.[1235] Zur weiteren Kritik an der großzügigen Zulassung der Verwertbarkeit rechtswidrig durch Private erlangter Informationen wird in Teilen der Literatur auf das „Hehlereiargument" zurückgegriffen: Im dortigen Kontext hat der Hehler dem Eigentümer die Sache zwar nicht selbst entwendet, dennoch wird die durch den Hehler geschaffene Perpetuierung der rechtswidrigen Situation durch die Rechtsordnung nicht milder bewertet als die entsprechende Vortat.[1236] Übertragen auf die hiesige Situation liegt in der Audioaufzeichnung zwar keine Straftat, gleichwohl kann die Quintessenz des Hehlereiarguments auf die hiesige Situation übertragen werden: Zwar hat der Staat die beweisgegenständliche Audioaufzeichnung nicht selbst generiert, dennoch perpetuiert dieser durch die Verwendung, die den Betroffenen in seinen Rechten verletzende Situation. Daran anknüpfend wollen vor allem die Vertreter der sog. Einheitsthese in Fällen der strafbewährten privaten Beweisgewinnung von einem Beweisverwertungsverbot ausgehen.[1237] Darüber hinaus finden sich in der Literatur eine Reihe an unterschiedlichen Ausgestaltungen zum Umgang mit rechtswidrig durch Private erlangten Beweismitteln. Während manche in der Verwertung solcher Informationen einen Verstoß gegen die Notwendigkeit eines fairen Verfahrens sehen,[1238] wollen andere analog § 136a StPO jedenfalls dann, wenn die private Geständniserlangung gegen § 136a StPO verstößt, von einem Beweisverbot ausgehen.[1239] Unabhängig der Qualität des für ein Beweisverbot geforderten Verhaltens

1235 Vgl. *Niehaus*, NZV 2016, 551, 552 zur anlasslosen Videoüberwachung des Straßenverkehrs; *ders*. DAR 2009, 632, 634.

1236 *Grundlach* in: AK-StPO, § 136a StPO, Rn. 13; *Schmidt-Leichner*, 46. DJT, Bd. 2, F 137, 139; *Schroeder/Verrel*, Strafprozessrecht, § 17, Rn. 132; *Hassemer/Matussek*, Das Opfer als Verfolger, S. 77; *Joerden*, JuS 1993, 927, 928; *Mende*, Grenzen privater Ermittlungen, S. 204 ff.; *Koriath*, Beweisverbote im Strafprozess, S. 102; *Sydow*, Kritik der Lehre von den Beweisverboten, S. 116.

1237 *Schmidt-Leichner*, 46. DJT, Bd. 2, F 137, 139; *Müssig*, GA 1999, 119, 138 f.; *Stoffer*, Privatisierung des strafprozessualen Ermittlungsverfahren, S. 479 f.

1238 *Kargl* in: NK-StGB, § 201 StGB, Rn. 28.

1239 *Eckhardt*, Private Ermittlungsbeiträge, S. 12 ff.; *Lesch*, GA 2000, 355, 369 ff.; FS-Stöckel/*Jahn*, 259, 280; *Gaede*, StV 2004, 46, 52; *Bung*, ZStW 2013, 536, 547.

Privater gehen die Vertreter einer Unverwertbarkeit – sofern die Voraussetzungen, die diese hierfür aufstellen erfüllt sind – davon aus, dass der Staat durch die Verwertung solcher rechtswidrig erlangter Beweismittel seine eigene Straflegitimation desavouieren würde.[1240]

Ebenso finden sich auch in der Literatur Stimmen, die die großzügige Beweisverwertung rechtswidrig gewonnener Beweismittel durch Private nicht beanstanden wollen.[1241] So sei es nicht Aufgabe des Verfahrensrechts Verfehlungen Privater zu ahnden.[1242] Diesbezüglich erfülle der Staat seine (Schutz-) Pflicht durch das Durchsetzen des gegen den Beweisbeschaffenden entstandenen Strafanspruchs.[1243] Da jedoch die materiellen Strafgesetze gegen die der Private womöglich verstößt, keinen beweisrechtlich relevanten Schutzzweck verfolgen, könne sich daraus auch kein staatliches Verwertungsverbot ergeben.[1244] Im Übrigen würde eine Relevanz des privaten Rechtsverstoßes theoretisch dazu führen können, dass eine Privatperson ein Beweismittel unter Inkaufnahme einer eigenen Strafbarkeit gerade deshalb rechtswidrig beschafft, um dessen Unverwertbarkeit im Strafprozess zu bezwecken.[1245]

cc) Strafbarkeit gem. § 201 Abs. 2 Nr. 1 StGB

Abschließend ist drauf hinzuweisen, dass die Aufzeichnung einer nicht autorisierten Audioaufzeichnung regelmäßig keine Strafbarkeit gem. § 201 Abs. 2 Nr. 1 StGB begründen wird. Auf Grundlage der im Gesetzgebungs-

1240 Vgl. *Stoffer*, Privatisierung des strafprozessualen Ermittlungsverfahren, S. 440.

1241 *Löffelmann*, Grenzen der Wahrheitserforschung, S. 221 f.; *Reeb*, Internal Investigations, S. 130; *Jäger*, GA 2008, 471, 493; *Kleinknecht*, NJW 1966, 1537, 1542; *Kaspar*, GA 2013, 206, 223.

1242 *Löffelmann*, Grenzen der Wahrheitserforschung, S. 221 f.; *Jäger*, GA 2008, 471, 493; *Kleinknecht*, NJW 1966, 1537, 1542; *Kramer*, Jura 1988, 520, 522; wenngleich die Fragwürdigkeit des Ergebnisses erkennend, dass die entsprechenden Informationen durch die Strafverfolgungsbehörden selbst nicht hätten erlangt werden können *Haffke*, GA 1973, 65, 83.

1243 *Jäger*, Beweisverwertung und Beweisverwertungsverbote, S. 223 f.; *Kaspar*, GA 2013, 206, 223.

1244 *Jäger*, Beweisverwertung und Beweisverwertungsverbote, S. 225; *ders.*, GA 2008, 471, 493; *Reeb*, Internal Investigations, S. 130; differenzierend mit dem Hinweis auf die leidende Rechtsstaatlichkeit, wenn Beweisergebnisse in die Hauptverhandlung eingeführt werden, die durch Straftaten gewonnen wurden, vgl. *Klug*, 46. DJT, Bd. 2, F 30, F 47.

1245 *Godenzi*, GA 2008, 500, 509.

verfahren verwendeten Definition eines Abhörgerätes, als besonderes Hilfsmittel, mit welchem *„das gesprochene Wort über dessen Klangbereich hinaus durch Verstärkung oder Übertragung unmittelbar wahrnehmbar*“ ist,[1246] ist das Endgerät des Betroffenen aufgrund der dadurch initiierten Übertragung der Aufzeichnung in die Cloud des Dienstleistungsanbieters, als Abhörgerät anzusehen. Dagegen verstand der BGH den Begriff des Abhörgerätes in einer älteren Entscheidung scheinbar enger und fasst hierunter den Einsatz verbotener technischer Mittel wie beispielsweise versteckt angebrachte Mikrofone, Richtmikrofone, drahtlose Kleinstsender sowie Vorrichtungen zum “Anzapfen” von Telefonleitungen.[1247] Angesichts des stetigen technischen Fortschritts widerspräche es jedoch dem § 201 StGB immanenten Schutzweck, Angriffe auf den geschützten Bereich der Persönlichkeit zu verhindern und die Kontrolle des Sprechenden über die Reichweite seiner Äußerungen zu gewährleisten[1248], wenn der Tatbestand auf bestimmte Gattungen technischer Geräte begrenzt würde.[1249] Vielmehr ist es erforderlich auch alltagsübliche Gegenstände, die beispielsweise mittels eines Mikrofons oder einer Kamera entsprechende Audioaufzeichnungen erzeugen können, als Abhörgerät i.S.d. § 201 Abs. 2 Nr. 1 StGB anzusehen.[1250] Jedenfalls erfordert die Tathandlung des Abhörens ein willensgesteuertes, gezieltes Verhalten.[1251] Ein „zufälliges Mithören“ eines Gesprächs kann somit allenfalls dann tatbestandsmäßig sein, wenn der Zuhörende für das Abhörgerät entweder verantwortlich ist oder es (versehentlich) eingeschaltet hat.[1252] An einem solchen Verhalten fehlt es in den hier zugrunde liegenden Fällen regelmäßig. Weder ist

1246 BT-Drs. IV/65O, S. 332.

1247 BGHSt 39, 335, 343; BGHZ, NJW 1982, 1397, 1398.

1248 BGHSt 39, 335, 343.

1249 *Fischer*-StGB, § 201 StGB, Rn. 7a.

1250 *Graf* in: MüKo-StGB, § 201 StGB, Rn. 32; *Eisele* in: Schönke/Schröder, § 201 StGB, Rn. 19; *Kargl* in: NK-StGB, § 201 StGB Rn. 17; a.A.: *Kühl* in: Lackner/Kühl, § 201 StGB, Rn. 5; *Hilgendorf/Valerius*, Internetstrafrecht, Rn. 426, die unter Rekurs auf die Besonderheit des technischen Mittels, Gegenstände die zur „Standardausstattung“, daher alltagsüblich sind nicht als Abhörgerät einstufen wollen. Einig ist man sich insofern jedenfalls, dass Telefone in ihrer normalen Verwendung keine Abhöreinrichtungen darstellen, selbst wenn infolge einer Fehlschaltung oder einer anderen technischen Störung ein Mithören fremder Gespräche möglich ist, vgl. *Graf* in: MüKo-StGB, § 201 StGB, Rn. 33.

1251 *Graf* in: MüKo-StGB, § 201 StGB, Rn. 31; *Wormer,* Der strafrechtliche Schutz der Privatsphäre, S. 199 f.; *Kargl* in: NK-StGB, § 201 StGB, Rn. 16; *Eisele* in: Schönke/Schröder, § 201 StGB, Rn. 20.

1252 *Graf* in: MüKo-StGB, § 201 StGB, Rn. 31.

„der Dienstleistungsanbieter“ oder der die Audioaufzeichnung abhörende Angestellte für das sich in der ausschließlichen Verfügungsgewalt des Betroffenen befindlichen Endgerät verantwortlich noch haben Angestellte des Dienstleistungsanbieter das Endgerät durch eine aktive Handlung (versehentlich) aktiviert. Zur Aktvierung des Sprachassistenten kam es erst durch das Zusammenspiel einer aus der Sphäre des Betroffenen herrührendes Signal, das durch den Sprachassistenten auf technischer Grundlage missverständlich gedeutet wurde.

dd) Stellungnahme

Zuzustimmen ist der Rechtsprechung an dieser Stelle in einem übergeordneten, grundsätzlicheren Punkt. Im Unterschied zur Ermittlung eines unselbstständigen Beweisverwertungsverbotes ist es bei der Ermittlung eines selbstständigen Beweisverwertungsverbotes – mangels anderweitiger, den gesetzgeberischen Willen unmittelbar zum Ausdruck bringender Vorschriften – grundsätzlich sachgemäß, auf die Abwägungsdoktrin zurückzugreifen.[1253] Gleichwohl ist auch in dieser Abwägung die überproportionale Gewichtung des Kriteriums der Tatschwere zur Ermittlung des Strafverfolgungsinteresses kritisch zu sehen. Ohne für ein vollständiges Außenvorlassen dieses Kriteriums streiten zu wollen,[1254] darf es auch im Rahmen der selbstständigen Beweisverwertungsverbote nicht angehen, dass dieses zum alleinentscheidenden Kriterium zugunsten einer Verwertbarkeit manipuliert wird.

Im Grunde zutreffend ist ferner, dass die Beweiserhebungsvorschriften der StPO sich nicht an Private, sondern lediglich an die Strafverfolgungsbehörden richten.[1255] Folglich kann der eigentliche Akt der rechtswidrigen und dadurch im Widerspruch zu der StPO stehenden privaten Beweisgewinnung nicht Anknüpfungspunkt etwaiger Beweisverwertungsverbote sein. Gerade sofern mangels staatlicher Beweiserhebung ohnehin ein selbstständiges Beweisverwertungsverbot im Raum steht, welches sich nur aus Verfassung ergeben kann, kann der rechtswidrige Beweiserhebungsakt hierauf keinen unmittelbaren Einfluss haben. Auch wenn die rechtswidrige private Beweisgewinnung folglich als unmittelbarer Anknüpfungspunkt für das Entstehen eines solchen Beweisverwertungsverbo-

1253 *Beulke*, ZStW 1991, 657, 678 f.
1254 so aber *Kassing*, JuS 2004, 675, 677.
1255 BGHSt 27, 355, 357; BGHSt 34, 39, 52; BVerfG, NJW 2011, 2417, Rn. 58.

tes ausscheidet, bedeutet dies nicht, dass dieser Makel nicht im Verfahren fortwirkt. Zu denken ist dabei an den hoheitlichen Akt der Verwertung eines solchen Beweismittels im Strafprozess, beispielsweise durch Abspielen der Audioaufzeichnung. Im Rahmen der hoheitlichen Verwertung eines rechtswidrig gewonnen Beweismittels kann nicht außer Acht bleiben, dass sich der Staat durch die Verwertung dieses Beweismittel dieses zwangsläufig zu eigen macht und die mit der Beweisgewinnung einhergehende Rechtsverletzung des Betroffenen perpetuiert. Eine vollständige Trennung zwischen der Beweiserhebung und der anschließenden Beweisverwertung ist auch an dieser Stelle schlicht nicht möglich.[1256] Hinzukommend stellt es sich in der hier vorliegenden Situation nicht nur derart dar, dass der Staat eine rechtswidrige Situation lediglich aufrecht erhält (dem Betroffenen stünde ein zivilrechtlicher Löschungsanspruch hinsichtlich der rechtswidrig aufgezeichneten Datei zu), d.h. den rechtswidrigen Zustand nicht beseitigt, sondern durch die staatliche Verwertung des Beweismittels gar auf dem durch die rechtswidrige Beweisgewinnung entstandenen Unrecht durch die Verwertung weiter aufbaut. Das Vorspielen der Audioaufzeichnung in der Verhandlung stellt daher einen neuen, nicht lediglich privaten, sondern staatlichen Eingriff in die grundrechtlich geschützten Rechte des Betroffenen dar.[1257] Es erscheint überdies inkonsequent, wenn sich der Staat dabei gewissermaßen das Beweisergebnis „herauspickt", während er mögliche damit durch die rechtswidrige Beweisgewinnung zusammenhängenden Rechtsverstößen schlicht ignorieren können soll.[1258] Dies gerade vor dem Hintergrund, dass die verfassungsrechtliche staatliche Pflicht der Wahrung der Rechtsordnung nicht nur das Verfolgen von Straftaten erfordert, sondern diese Pflicht auch die Gewährleistung eines effektiven Grundrechtsschutzes – der freilich auch dem Angeklagten Straftäter zusteht – umfasst. Diese auch gegenüber Zugriffen Privater bestehende staatliche Schutzpflicht wäre unvollständig, wenn Rechtsverstöße Privater prozessrechtlich gebilligt würden.[1259] Zur Vermeidung dessen ist der Makel der Beweiserlangung, deren Ergebnisse sich der Staat nun zu Nutze macht, im Rahmen der verfassungsrechtlichen Rechtfertigung des mit der Verwer-

1256 Vgl. FS-Beulke/*Bung/Huber*, 655, 666.
1257 *Beulke* in: SSW-StPO, Einleitung, Rn. 321; vgl. *Wölfl*, Verwertbarkeit heimlicher privater Ton- und Bildaufnahmen, S. 108; *Cornelius*, NJW 2016, 2282, 2283.
1258 So auch *Niehaus*, NZV 2016, 551, 552, a.A.: *Jansen*, StV 2019, 578, 584.
1259 *Wolter* in: SK-StPO, § 136a StPO, Rn 13.

tung des bemakelten Beweismittels einhergehenden Grundrechtseingriff zu berücksichtigen.[1260]

Sollte sodann die hoheitliche Verwendung eines rechtswidrig durch Private hervorgebrachte Beweismittels mit einem Beweisverwertungsverbot belegt sein, hat dies auch nichts mit einem – dem deutschen Strafprozessrecht in der Tat fremden – Disziplinierungsgedanken zu tun,[1261] sondern verhindert schlicht, dass das mit der Beweisgewinnung begonnene private Unrecht sich in einem staatlichen Urteil zum Nachteil des Beschuldigten manifestiert. Die Möglichkeit, den strafrechtswidrig Beweismittel Beschaffenden selbst zu sanktionieren, vermag hieran nichts zu ändern,[1262] denn dadurch würde lediglich das durch den Beweisbeschaffenden begangene Unrecht bestraft, nicht jedoch verhindert, dass dieses Unrecht in der hoheitlichen Beweisaufnahme erneut zu Tage tritt.

Anknüpfend daran soll der Umgang mit zielgerichtet rechtswidrig durch Private gewonnenen Beweismittel dahingehend modifiziert werden, dass zur Rechtfertigung des durch die Verwertung eines solchen Beweismittels erfolgten Grundrechtseingriffes und der damit korrespondierenden Entstehung eines (aus dem nicht zu rechtfertigenden Grundrechtseingriff folgenden) selbstständigen Beweisverwertungsverbotes erst auf einer „dritten Stufe“ auf eine Abwägung zurückgegriffen wird. Ausgehend von der drei-Sphären Theorie muss dabei erstens analog zum Kernbereich bei der Betroffenheit der Intimsphäre eine Rechtfertigung des mit der Verwertung einhergehenden Grundrechtseingriffes in das Recht auf informationelle Selbstbestimmung stets abgelehnt werden und folglich ein selbstständiges Beweisverwertungsverbot angenommen werden.[1263] Bringen die privat erlangten Beweismittel mithin Informationen hervor, die in diese Sphäre einzuordnen sind, scheidet eine staatliche Verwertung in jedem Falle aus. Auch hier ist unter Einbeziehung der obigen Ausführungen zu beachten, dass ein Straftatenbezug in bestimmten Fällen (Selbstgespräch, beichtende / reflektierende Zwiegespräche) nichts an einer Zuordnung

1260 *Grünwald*, Das Beweisrecht, S. 163; *Götting*, Beweisverwertungsverbote in Fällen nicht geregelter Ermittlungstätigkeit, S. 298.

1261 *Gropp*, StV 1989, 216, 218, der unter einem Verweis darauf, dass die Disziplinierung der staatlichen Strafverfolgungsorgane nicht primäres Anliegen, sondern allenfalls Reflex der Verwertungsverbote ist, folgert, dass auch bei einer rechtswidrigen Beweisgewinnung durch Private kaum Lockerungen hinsichtlich der Verwertbarkeit anerkannt sind.

1262 So aber *Störmer*, Grundlagen der Verwertungsverbote, S. 118.

1263 *Müssig*, GA 1999, 119, 138, Fn. 67; *Gless* in: LR-StPO, § 136a StPO, Rn. 12; *Bockemühl*, Private Ermittlungen im Strafprozess, S. 125 ff.

zur Intimsphäre zu ändern vermag. Während die Rechtsprechung sodann in jeglichen Fällen, die lediglich die Privatsphäre betreffen, in eine Abwägung zwischen dem Strafverfolgungsinteresse und der Intensität des Grundrechtseingriffs eintreten würde, soll dies – nach der hier vorgeschlagenen Lösung – erst nach einem weiteren Zwischenschritt geschehen. Hinsichtlich der Beweiserlangung durch Private sind zwei Fälle zu unterscheiden.

Zum einen die strafbare Beweiserlangung durch Private und zum anderen die lediglich rechtswidrige, aber nicht strafbewährte Beweiserlangung durch Private. Während im ersten Fall eine Verwertbarkeit des so erlangten Beweismittels ebenfalls abwägungsresistent ausscheiden muss (mithin also der durch die staatliche Verwertung eines solchen Beweismittels ausgelöste Grundrechtseingriff nicht gerechtfertigt werden kann und damit erneut ein selbstständiges Beweisverwertungsverbot entstehen muss), kann lediglich im Falle einer einfach rechtswidrigen Beweiserlangung durch Private auf die Abwägungslehre zur Rechtfertigung des Grundrechtseingriffes zurückgegriffen werden.[1264] Für die Unabwägbarkeit im Falle der strafrechtswidrigen Beweiserlangung[1265] spricht, dass wenn der Staat mittels seines schärfsten Schwertes, des Strafrechts, strafrechtswidriges Ver-

1264 In diese Richtung geht auch die Abstimmung des 67. Dt. Juristentages (2008) in welcher sich eine klare Mehrheit der Teilnehmer für ein Beweisverwertungsverbot aussprachen, wenn die Erkenntnisse von Privatpersonen mit strafbaren Mitteln erlangt wurden. Für den Fall, in dem die Beweise durch Private mit sonstigen rechtswidrigen Mitteln erlangt wurden, sprach sich dagegen eine knappe Mehrheit gegen ein Beweisverwertungsverbot aus, vgl. Beschlüsse des 67. Dt. Juristentages, Band II, L. 70; *Niehaus*, NZV 2016, 551, Fn. 22; *Müssig*, GA 1999, 119, 138 f.; *Stoffer*, Privatisierung des strafprozessualen Ermittlungsverfahren, S. 479 f.; a.A.: *Traub*, Verwertbarkeit von Selbstgesprächen, S. 165; *Jäger*, GA 2008, 473, 493; *Kaspar*, GA 2013, 206, 211; *Rogall*, JZ 2008, 818, 828; *Löffelmann*, Grenzen der Wahrheitserforschung, S. 221 f.

1265 Von einer strafrechtswidrigen Beweiserlangung durch Private soll nach dem hier zugrunde gelegten Verständnis nur dann ausgegangen werden, wenn der Private das spätere Beweismittel tatsächlich unter einem Verstoß gegen strafrechtliche Normen *erlangt*. Keine strafrechtswidrige *Erlangung* des Beweismittels liegt der Verwertung einer Zeugenaussage zugrunde, die unter Verstoß gegen eine materiell-rechtliche Schweigepflicht (§ 203 StGB) getätigt worden ist. Somit ist über die Verwertbarkeit losgelöst von der Thematik der rechtswidrigen Beweisgewinnung durch Private und vielmehr am Maßstab des § 53 StPO zu entscheiden. Es handelt sich nicht um ein durch Private strafrechtswidrig erlangtes Beweismittels, sondern um eine (rechtswidrige) Offenlegung von rechtmäßig erlangtem Wissen, ähnlich auch *Freund*, GA 1993, 49, 56; a.A..: *Rogall*, JZ 2008, 818, 828, *Neuber*, Beweisverwertungsverbote im Strafprozess, S. 157. Über die Verwertung des unter Verstoß gegen §§ 53 StPO, 203 StGB zu-

halten sanktioniert, er sich nicht ebenfalls strafrechtswidrig erlangtes Beweismittel zu Nutze machen darf. Wer die Strafverfolgung – zu Recht – als eines der obersten Verfassungsziele betrachtet, darf zu dessen Durchsetzung nicht selbst auf solche, dieses Verfassungsziel erst notwendig machende strafrechtswidrige Handlungen, zurückgreifen. Die Verwertung solcher Beweismittel würde darüber hinaus einer Privatjustiz in Form privater Beweisermittlungen erheblich Vorschub leisten. Die Begrenzung der Unverwertbarkeit auf die skizzierten krassen Ausnahmefälle kann der kriminalpolitisch und verfassungsrechtlich unerwünschten Situation privater Ermittlungen heute nicht mehr sachgerecht Einhalt gebieten. Da die Ermittlungsarbeit ausschließlich in der Hand des Staates liegt, muss eindeutig geregelt sein, dass strafrechtswidrig erlangte Beweismittel keine prozessuale Berücksichtigung finden. Ein Rückgriff auf das durch das StGB als strafbar normierte Verhalten berücksichtigt dabei dahingehend den gesetzgeberischen Willen, der durch die Pönalisierung verschiedener Verhaltensweisen zum Ausdruck bringt, dass ein solches Verhalten in einem Rechtsstaat nicht geduldet werden darf. Insofern entschied sich der Gesetzgeber bewusst dazu verschiedene Handlungen als Straftat, bloße Ordnungswidrigkeit oder lediglich mit zivilrechtlichen Unterlassungsansprüchen einzuordnen. Dies darf durch die staatliche Verwertung im Widerspruch hierzu generierter Beweismittel nicht missachtet werden. Erst auf einer dritten Stufe ist sodann im Falle eines nicht strafrechtswidrig erlangten Beweismittels in eine Abwägung zwischen den kollidierenden Interessen einzutreten.

Der hier gebildete Fall wäre demnach mangels eines strafrechtswidrig erlangten Beweismittels auf der dritten Stufe im Rahmen einer Abwägung zu entscheiden. Durch das Vorschalten zweier weiterer, der Abwägung entzogenen Stufen, wird ferner erreicht, dass das Kriterium der Tatschwere in diesen Fällen nicht per se zur Verwertbarkeit führen kann. Auf der dritten Stufe erscheint es sodann sachgerecht, bei gravierenden, im Prozess zu beurteilenden Straftaten nicht strafrechtswidrig erlangte Beweismittel zur Verwertung zuzulassen. Rechtsicherer Anhaltspunkt könnte an dieser Stelle der Straftatenkatalog nach den §§ 100c Abs. 1 Nr. 1, 100b Abs. 2 StPO bieten, da der Gesetzgeber solche Straftaten als gewichtig genug einordnete, um rechtmäßig innerhalb eines Wohnraums das durch Art. 13 GG und durch das allgemeine Persönlichkeitsrecht geschützte Wort abzuhören. Liegt ein solcher Fall vor, wäre der mit der Verwertung einhergehende

---

stande gekommenen Beweismittels ist daher unter Schutzzweckgesichtspunkten zu entscheiden, vgl. *Beulke/Swoboda*, Strafprozessrecht, Rn. 710.

neue staatliche Grundrechtseingriff in das allgemeine Persönlichkeitsrecht gerechtfertigt. Ein selbstständiges Beweisverwertungsverbot würde in diesem Fall folglich nicht entstehen.

d) Übermittlung etwaiger Hintergrundäußerungen Dritter während autorisierter Aufzeichnung

Fraglich ist zudem, wie sich die Verwertbarkeit in der Situation darstellt, in der die durch den Dienstleistungsanbieter übermittelten Aufzeichnungen Hintergrundgespräche Dritter im Rahmen autorisierter Aufzeichnungen durch den Nutzer beinhalten. So ist vorstellbar, dass während der Nutzer den Sprachassistenten bittet, gewisse Nahrungsmittel auf den Einkaufszettel zu schreiben, eine weitere sich im Raum befindliche Person erzählt, wie ihr Ehemann seit Jahren Steuern hinterzieht. Die Rechtsprechung geht bei der Aufzeichnung etwaiger Hintergrundgespräche im Kontext einer Überwachung gem. § 100a StPO von einer Verwertbarkeit der so erlangten Informationen aus.[1266] Da bereits Hintergrundgespräche im Rahmen der Telefonüberwachung, die eigentlich nur die abgehörte Telefonverbindung umfasst, verwertbar sein sollen, ist anzunehmen, dass dies erst Recht für Hintergrundgeräusche gilt, die ein Sprachassistent aufzeichnete. Denn der Sprachassistent zeichnet nach seiner Aktivierung bekanntermaßen sämtliche ablaufende Gespräche auf und ermöglicht damit bereits seiner Funktion nach, eine breiter gestreute Aufnahme. Dennoch eignet sich die Entscheidung nicht zur Übertragung auf die hiesige Situation. Während im Falle der Hintergrundgeräusche im Rahmen des § 100a StPO durchaus diskutiert werden kann, ob die Verwertbarkeit solcher Informationen die richterlich angeordnete Telekommunikationsüberwachung nach § 100a StPO, „zum großen Lauschangriff gem. § 100c StPO mutieren“ lässt,[1267] ist diese Diskussion hier nicht zielführend. Schließlich handelt es sich um eine Aufzeichnung, die vollkommen losgelöst etwaiger staatlich angeordneter Überwachungsmaßnahmen stattfindet. Vor dem Hintergrund einer möglicherweise rechtswidrigen Beweisgewinnung durch Private ist daher auch in diesem Beispielsfall zur weiteren Beurteilung entscheidend, ob insofern ein Einverständnis zur Aufzeichnung vorliegt. Das Einverständnis muss, sofern mehrere Personen von einer Auf-

1266 BGH, NStZ 2008, 473; BGH NStZ 2018, 550, 551.
1267 vgl. *Prittwitz*, StV 2009, 437.

zeichnung betroffen sind, stets von sämtlichen Personen erteilt werden.[1268] Dabei könnte in dem lauten Sprechen einer dritten Person, während sich eine weitere Person in einer Interaktion mit einen Sprachassistenten befindet, eine konkludente Inkaufnahme des Risikos der Aufzeichnung des eigenen Wortes und mithin ein konkludent erteiltes Einverständnis zu erblicken sein. Zwar ist korrekt, dass nicht jede Kenntnis des Sprechers von einer Aufnahme automatisch bedeutet, dass dieser mit derselben einverstanden ist.[1269] Jedenfalls aber, wenn dem Betroffenen ohne nachteilige Konsequenzen die Möglichkeit offensteht, seine verbale Artikulation aufgrund der Gefahr einer Aufzeichnung zu unterbrechen, kann von einer Gleichgültigkeit im Sinne eines Einverständnisses auszugehen sein.[1270]

Problematisch ist jedoch, wie sich die Situation darstellt, wenn die Dritte Person nicht weiß, dass ein aktivierter Sprachassistent auch etwaige, während einer Spracheingabe im Raum vernommene, Hintergrundgespräche aufzeichnet. Sofern keine Kenntnis einer ablaufenden Aufzeichnung vorliegt, kann logischerweise auch keine, ein konkludentes Einverständnis begründende, Gleichgültigkeit vorliegen. Entscheidend ist in der vorliegenden Situation folglich, ob die Dritte Person Kenntnis von der technisch erfolgten Aufzeichnung bei der Nutzung eines Sprachassistenten hatte. Sofern dies zu bejahen ist, wird hierin regelmäßig ein konkludentes Einverständnis zu erblicken sein, womit die Situation analog zu der unter b) dargestellten Situation zu behandeln ist. Fehlt es an dieser Kenntnis, handelt es sich um eine unbefugte Aufzeichnung i.S.d. § 201 Abs. 1 Nr. 1 StGB, womit die Situation anhand der unter c) entwickelten Maßstäbe zu behandeln ist. Ob beim konkret Betroffenen letztlich von einer solchen Kenntnis auszugehen ist, muss der tatrichterlichen Entscheidung obliegen.

e) Exkurs: Richterliche Strafbarkeit durch Verwertung nach § 201 Abs. 1 Nr. 2 StGB

Nicht außen vor bleiben soll an dieser Stelle, dass das Vorspielen der Audioaufzeichnung im öffentlichen Strafprozess gar eine eigene Strafbarkeit begründen könnte, wenn es sich um – wie hier – gegen § 201 Abs. 1 Nr. 1 StGB verstoßende Aufnahmen handelt und die Verwertung als Be-

1268 *Eisele* in: Schönke/Schröder, § 201 StGB, Rn. 13; *Graf* in: MüKo-StGB, § 201 StGB, Rn. 41; *Schünemann* in: LK-StGB, § 201 StGB, Rn. 10.
1269 *OLG Thüringen*, NStZ 1995, 502, 503.
1270 Vgl. *OLG Thüringen*, NStZ 1995, 502, 503.

weismittel im Strafverfahren als Gebrauchen i.S.d. § 201 Abs. 1 Nr. 2 StGB, einzuordnen wäre.[1271] Dies erscheint allerdings aus zwei Punkten problematisch. Zum einen ist zu klären, ob es sich bei der „so hergestellten Aufnahme" nach Nummer 1 um eine vorsätzlich hergestellte Aufnahme handeln muss und zum anderen, ob die staatliche Verwertung möglicherweise nicht unbefugt bzw. gerechtfertigt im Sinne derer die das Merkmal „unbefugt" nicht zum Tatbestand zählen wollen,[1272] geschieht. Mangels der Strafbarkeit nicht vorsätzlicher Audioaufzeichnungen und da eine solche Situation vor dem Einzug diverser Sprachassistenten in den Alltag der Bürger nur schwer vorstellbar war, findet sich hierzu naturgemäß keine Diskussion in Rechtsprechung und Literatur. Ausgehend vom Wortlaut des § 201 Abs. 1 Nr. 2 StGB der von einer „so hergestellten Aufnahme" spricht, ist anzunehmen, dass dies die äußeren, daher objektiven Umstände, der Aufnahme meint. Die subjektive Sicht des Täters entscheidet zwar mit über dessen persönliche Strafbarkeit, dem Wortlaut nach ist für die Verwirklichung des § 201 Abs. 1 Nr. 2 StGB jedoch irrelevant, ob die Herstellung der i.S.d. § 201 Abs. 1 Nr. 2 StGB „gebrauchten" Aufnahme vorsätzlich erfolgte. Entscheidend ist allein eine im objektiven Sinne rechtswidrig angefertigte Aufnahme.[1273] In systematischer Hinsicht spricht hierfür, dass es sich bei § 201 Abs. 1 Nr. 2 StGB im Verhältnis zu § 201 Abs. 1 Nr. 1 StGB um keine Qualifikation, sondern einen eigenen Straftatbestand handelt, der eine von § 201 Abs. 1 Nr. 1 StGB losgelöste Handlung unter Strafe stellt. Auch telelogische Gesichtspunkte sprechen dafür, für das Verwirklichen des § 201 Abs. 1 Nr. 2 StGB keine vorsätzlich hergestellte Aufzeichnung zu verlangen. Der Schutzzweck des § 201 Abs. 1 Nr. 2 StGB, das Gebrauchen jeglicher nichtöffentlicher Kommunikation durch Pönalisierung zu vermeiden,[1274] besteht unabhängig davon, ob die ursprüngliche Aufzeichnung vorsätzlich erfolgte oder nicht. In dem

1271 Vgl. BayObLG, NJW 1990, 197, 198; *Kramer*, NJW 1990, 1760; 1763, *Wohlers*, JR 2016, 509, 512; FS-Kleinknecht/*Otto*, 319, 338; *Brunhöber*, GA 2010, 571, 586.

1272 Vgl. *Heuchemer/Paul*, JA 2006, 616, 619 m.w.N.

1273 Vgl. *Graf* in: MüKo-StGB, § 201 StGB, Rn. 25 zum in der Literatur herrschenden Streit, ob sich das Merkmal einer „so hergestellte Aufnahme" nur auf die näheren Umstände der Aufzeichnung gemäß Nr. 1 bezieht oder die Verweisung auch das vorangestellte Merkmal „unbefugt" beinhaltet. Da die Aufnahme hier nach allen zur Lesart des Unbefugtheitsbegriff vertretenen Ansichten jedoch ohnehin unbefugt erfolgte, ist diese Auseinandersetzung nicht von Bedeutung.

1274 *Graf* in: MüKo-StGB, § 201 StGB, Rn. 3.

einen wie dem anderen Fall würde das Gebrauchen, einer unter Verwirklichung des objektiven Tatbestands des § 201 Abs. 1 Nr. 1 StGB hergestellten Aufzeichnung, schließlich auch eine Verletzung des zu schützenden Rechtsguts auf Seiten des Betroffenen darstellen. Der Strafbarkeit des Richters kann jedoch entgegenstehen, dass das Gebrauchen der Aufzeichnung durch Verwenden im Strafprozess befugt geschieht. Der Beantwortung dieser Frage werden im Ergebnis die gleichen Überlegungen zu Grunde liegen, wie der Frage, ob der mit dem Vorspielen eines rechtswidrig durch einen Privaten erlangten Beweismittels einhergehende staatlichen Eingriff in das allgemeine Persönlichkeitsrecht des Betroffenen gerechtfertigt werden kann.[1275] Letztlich wird es aber regelmäßig nicht dazu kommen, dass auf Grund eines staatlichen Verstoßes gegen § 201 Abs. 1 Nr. 2 StGB ein Beweisverwertungsverbot Bedeutung erlangen würde.[1276] Denn auch in diesem Fall kommt im hiesigen Kontext vorgeschaltet bereits die Frage nach dem Umgang mit der rechtswidrig durch einen Privaten erlangten Audioaufzeichnung auf. Ist die Audioaufzeichnung nicht mit einem Beweisverwertungsverbot belegt, so erfolgt das Abspielen der entsprechenden Audioaufzeichnung im Prozess befugt i.S.d. § 201 Abs. 1 Nr. 2 StGB. Mit anderen Worten ist die strafprozessuale Verwertung dann als im Einklang mit den Vorschriften der StPO stehend ohnehin nicht zu beanstanden. Erst wenn der Richter eine Audioaufzeichnung trotz eines offensichtlich bestehenden Beweisverbotes in den Prozess einführt, kommt § 201 Abs. 1 Nr. 2 StGB hinsichtlich dessen materieller Strafbarkeit Bedeutung zu. Für das Entstehen eines Beweisverbotes hat dies jedoch keine Bedeutung mehr, da sich dieses in den hier relevanten Fragestellungen – unabhängig von einer nochmaligen „staatlichen" Strafbarkeit des Richters – bereits als Konsequenz aus dem (auf der strafrechtswidrigen privaten Beweiserlangung aufbauenden) nicht zu rechtfertigenden Grundrechtseingriffs in das allgemeine Persönlichkeitsrecht in Form der hoheitlichen Verwertung ergibt.[1277]

1275 vgl. BayObLG, NJW 1990, 197, 198, das ausführt, dass die Verwertung einer heimlich durch einen Privaten hergestellten Tonbandaufnahme gegen § 201 Abs. 1 Nr. 2 StGB sowie das allgemeine Persönlichkeitsrecht verstoßen würde und eine Verwertung des Tonbandes im Wege eines Augenscheins daher nur unter strengen Verhältnismäßigkeitsvoraussetzungen in Betracht kommen könne; FS-Kleinknecht/*Otto*, 319, 338; *Brunhöber*, GA 2010, 571, 587 f.

1276 *Wölfl*, Verwertbarkeit heimlicher privater Ton- und Bildaufnahmen, S. 153.

1277 Vgl. dazu BGHSt 36, 167, 174, der ebenfalls unterscheidet, ob aufgrund der rechtswidrigen Erlangung eines Beweismittels durch Private, bei aber rechtmäßiger Beweiserhebung durch den Staat (bspw. durch eine Beschlagnahme) ein

III) Zwischenergebnis

Sofern das Gesetz ein unselbstständiges geschriebenes absolutes Beweisverwertungsverbot normiert, hat der Gesetzgeber die Unverwertbarkeit entsprechender Informationen zu Lasten des Beschuldigten abschließend beantwortet. Ist dagegen entscheidend, ob aus einem Verfahrensverstoß ein unselbstständiges ungeschriebenes Beweisverwertungsverbot entsteht, sollte – entgegen der Rechtsprechung – nicht auf eine Abwägungsentscheidung, sondern zur Wahrung des gesetzgeberischen Willens auf die Schutzzwecktheorie abgestellt werden. Zur Vermeidung glücklicher, ungerechtfertigter Fügungen zugunsten des Betroffenen kann gleich des dadurch hervorgebrachten Ergebnisses durch eine restriktive Anwendung der Grundsätze des hypothetisch rechtmäßigen Ermittlungsverlaufes, unter Beachtung des Normzwecks der missachteten Vorschrift, unter Umständen eine Verwertbarkeit zu bejahen sein.[1278] Hinsichtlich der Entstehung eines selbstständigen Beweisverwertungsverbotes ist zunächst zu sehen, dass beim Zugriff auf einen Sprachassistenten insbesondere die verfassungsrechtlichen Rechte aus Art. 10 GG, 13 GG und aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG vielfach betroffen sind. Sofern unter Zugrundelegung der 3-Sphären-Theorie ein Eingriff in die Intimsphäre erfolgt oder ein Eingriff in die Privat- oder Sozialsphäre nicht gerechtfertigt werden kann, hat dies ein selbstständiges Beweisverwertungsverbot zur Folge. Ein solches kann in bestimmten Fallkonstellationen insbesondere auch dann entstehen, wenn die Verwertung erst durch die unaufgeforderte Übermittlung der Audioaufzeichnungen durch den Dienstleistungsanbieter ermöglicht wird. Hier ist zu sehen, dass – auch wenn die Normen der StPO keine Bindungswirkung für Private entfalten – der durch diese im Rahmen der Beweisgewinnung begangene Verstoß gegen die Rechtsordnung durch die staatliche Verwertung im Strafprozess fortwirkt und dadurch zusätzlich eine staatliche Beeinträchtigung der Rechte des Angeklagten eintritt. Bei der Benutzung eines Sprachassistenten ist daher von besonderer Bedeutung, ob der Betroffene durch die Aktivierung des

---

Beweisverbot entstehen soll oder ob dies hinsichtlich eines von staatlichen Strafverfolgungsorganen rechtswidrig gewonnenes Beweismittel zu entscheiden ist. Zur Frage, ob ein *staatlicher* Verstoß gegen materiell-rechtliche Vorschriften im Rahmen der Beweisbeschaffung zu einem Beweisverbot führt, vgl. bejahend FS-Kleinknecht/*Otto*, 319, 338; *Beulke/Swoboda*, Strafprozessrecht, Rn. 733; *Trüg/Habetha*, NJW 2008, 887, 890 bei Straftaten, „die final angelegt sind auf die Beweismittelgewinnung"; ablehnend *Kaspar*, GA 2013, 206, 211.

1278 Vgl. auch *Beulke*, JURA 2008, 653, 661.

Sprachassistenten sein Einverständnis mit der notwendigen Speicherung der Informationen erteilte. Fehlt es an dieser Aktivierung ist – die Kernbereichsrelevanz der Aufzeichnungen ausgenommen – entscheidend, ob die Privatperson, daher der Dienstleistungsanbieter, durch die Aufzeichnung strafrechtswidrig oder lediglich gemessen an der übrigen Rechtsordnung rechtswidrig in den Besitz der Audioaufzeichnung gelangt ist. Entgegen der Rechtsprechung kann sodann lediglich im Falle einer bloß rechtswidrigen Beweiserhebung durch Private mittels einer Abwägung über das Entstehen eines selbstständigen Beweisverwertungsverbotes entschieden werden. Dieser letztgenannte Fall wird, mangels einer vorsätzlichen entgegen dem Einverständnis des Nutzers erfolgten Aufzeichnung, bei der privaten Beweiserlangung über einen Sprachassistenten vorliegen.

IV) Die Disponibilität eines Beweisverwertungsverbotes

Die durch einen Sprachassistenten den Strafverfolgungsbehörden zugänglich gemachten Informationen, können neben belastenden Inhalten auch solche zur Entlastung des Betroffenen enthalten. Gerade ein über einen Smart Speaker abgehörtes Wohnraumgespräche, kann eine Vielzahl an Informationen enthalten, die für den Betroffenen der Abhörmaßnahme womöglich entlastend wirken können.

1) Verwertbarkeit des Beweismittels zur eigenen Entlastung

Ist nach dem Gesagten grundsätzlich ein Beweisverbot angezeigt, stellt sich die anschließende Frage nach dessen Absolutheit. Gerade sofern ein unselbstständiges geschriebenes absolutes Beweisverwertungsverbot vorliegt, ist zu klären, ob dieses letztlich der Disposition des Angeklagten unterliegt. Dem liegt die Frage zu Grunde, ob ein solches Beweisverwertungsverbot auch die Verwertung als Entlastungsbeweis ausschließen soll. Um die Frage einer dogmatisch hinreichenden Antwort zuzuführen, muss dies im Lichte des konkret im Raum stehenden Beweisverbotes betrachtet werden. So erachtet die Rechtsprechung seit Jahren bei einem unselbstständigen ungeschriebenen Beweisverwertungsverbot ein Widerspruch zur Entstehung eines Beweisverbotes für erforderlich.[1279] Dieses primär der Ver-

1279 BGHSt 38, 214, 225 f. (fehlende Belehrung gem. § 136 Abs. 1 S. 2 StPO); BGHSt 42, 15, 23 (unterbliebener Hinweis auf das Recht zur Verteidigerkon-

fahrensförderung dienende Widerspruchserfordernis bringt als Kehrseite mit sich, dass der Angeklagte die Verwertung eines entsprechenden Beweismittels, in welchem er einen Entlastungsbeweis erblickt, durch einen Verzicht auf einen etwaigen Widerspruch in den eigenen Händen hält.[1280] Problematischer wird dies, sofern ein unselbstständiges geschriebenes absolutes Beweisverwertungsverbot (bspw. § 100d Abs. 2 oder auch § 136a Abs. 2 S. 2 StPO) im Raum steht. In diesen Fällen schließt der eindeutige Wortlaut die Notwendigkeit eines Widerspruchs durch den Beschuldigten aus.[1281] Zu Recht wird damit dem in der Rechtsprechung anklingenden Gedanken, auch bei solchen geschriebenen absoluten Beweisverwertungsverboten die Widerspruchslösung für anwendbar zu erachten, entgegengetreten.[1282]

Fraglich ist allerdings die damit scheinbar einhergehende Konsequenz, dass dem Beschuldigen somit auch seine Dispositionsbefugnis über ein solches Beweismittel genommen ist. Gerade vor dem Hintergrund eines den Kernbereich schützenden absoluten Beweisverwertungsverbotes aus § 100d Abs. 2 StPO ist denkbar, dass in solchen dem Kernbereich zuzuordnenden Gesprächen, vielmals auch entlastende oder jedenfalls strafmildernde Inhalte zur Sprache kommen.[1283] In diese Richtung geht auch die Rechtsprechung des Ersten Senats des BGH. Während dieser noch im Falle des in einem Krankenzimmer erfolgten Selbstgespräches bei der Betroffenheit des Kernbereichs eine Verwertung zu Lasten des Angeklagten explizit ausschloss, das Untersagen der Verwertung entlastender Hinweise jedoch als „*schwerlich vorstellbar*" bezeichnete,[1284] entschied sich der Erste Senat in einer späteren Entscheidung ausdrücklich auch bei einer Berührung des Kernbereichs für die Disponibilität eines Verwertungsverbots[1285]. Nicht gefolgt ist dieser Rechtsprechungslinie der Zweite Senat des BGH, der

---

sultation, §§ 136 Abs. 1 S. 2, 137 StPO); BGH NStZ 1996, 2020 (umgangene Belehrung durch das Einschalten eines V-Mannes); BGH, StV 2001, 545 (fehlende Katalogtat im Rahmen des § 100a StPO); BayObLG, StV 2002, 179 (unterbliebene Belehrung des früheren Zeugen und späteren Angeklagten bei Personenidentität nach § 55 Abs. 2 StPO).

1280 Zur Kritik an der höchstrichterlichen Widerspruchslösung, vgl. *Roxin/Schünemann*, Strafverfahrensrecht, § 24, Rn. 34; *Heinrich*, ZStW 2000, 398, 412; *Ventzke*, StV 1997, 543, 547; *Dornach*, NStZ 1995, 57, 61; *Widmaier*, NStZ 1992, 519, 521.

1281 *Fezer,* StV 1997, 57 f.; *Bruns* in: KK-StPO, § 100d StPO, Rn. 46.

1282 BGH, NStZ 1996, 290.

1283 Vgl. BVerfGE 109, 279, 369.

1284 BGHSt 50, 206, 215.

1285 BGHSt 51, 1, 4, Rn. 10.

in seiner Entscheidung zur strafprozessualen Handhabung eines Selbstgespräches zwar auch von dessen ausnahmsloser Zugehörigkeit zum Kernbereich ausging, sich dabei allerdings für eine umfassende und absolute Geltung des hieraus folgenden Beweisverwertungsverbotes aussprach.[1286] Aus §§ 100a Abs. 4 S. 2, 100c Abs. 5 S. 3 StPO a.F. folge der gesetzgeberische Wille wonach ein aus der Kernbereichsbetroffenheit resultierendes Beweisverwertungsverbot nicht nur als Belastungsverbot, sondern als „*jede Verwendung […] im Strafverfahren*" ausschließendes Beweisverwertungsverbot und damit auch als Entlastungsverbot zu verstehen sei.[1287] Dies verdeutliche das Bestrebens die Prozesslage so zu gestalten, als wäre der Eingriff in den privaten Kernbereich nie geschehen.[1288] Eine Unterscheidung zwischen Belastungs- und Entlastungsbeweis sei daher abzulehnen.[1289]

Gegen eine solche Sichtweise spricht jedoch, dass der das Verwertungsverbot bei einer Kernbereichsbetroffenheit normierende § 100d StPO n.F. im Unterschied zu § 136a Abs. 3 StPO gerade nicht davon spricht, dass ein solches Beweismittel auch bei einer Einwilligung durch den Betroffenen nicht verwendet werden darf.[1290] Selbst wenn die Gesetzesbegründung § 100c Abs. 5 S. 3 StPO a.F. als „absolutes Verwertungsverbot"[1291] einordnet, ist dies nicht gleichbedeutend damit, dass der Gesetzgeber die Verwertung auch in Form einer Entlastung des Angeklagten verbieten wollte. Vielmehr wird diese Absolutheit derart zu verstehen sein, dass die Unverwertbarkeit zu Belastungszwecken frei von etwaigen Abwägungsvorgängen sein soll und lediglich in diesem Sinne „absolut" ist. Die Bezeichnung als absolutes Beweisverwertungsverbot sollte in diesem Zusammenhang den Unterschied zu einem in §§ 100d Abs. 5 S. 2, 160a Abs. 2 S. 1, 3 StPO normierten unselbstständigen relativen Beweisverwertungsverboten verdeutlichen. Und in der Tat würde es befremdlich erscheinen,

1286 BGHSt 57, 71. 78, Rn. 21.
1287 BGHSt 57, 71, 78, Rn. 21; zustimmend *Mitsch*, NJW 2012, 1486, 1488 f.
1288 *Mitsch*, NJW 2012, 1486, 1488 f.
1289 *Schmitt* in: Meyer-Goßner/Schmitt, Einl., Rn. 55a; *Radtke* in: Radtke/Hohmann, Einl., Rn. 85; *Wollweber*, wistra 2001, 182; *Küpper*, JZ 1990, 416, 418.
1290 *Ladiges*, StV StV 2012, 517 f.; teilweise wird sogar hinsichtlich § 136a Abs. 3 S. 2 StPO vertreten, dass im Wege einer teleologischen Reduktion auch in diesen Fällen die Verwertbarkeit in den Händen des Betroffenen liegen müsse, *Roxin//Schäfer/Widmaier*, StV 2006, 655, 656; *Roxin*, StV 2009, 113, 114; *Jahn/Geck*, JZ 2012, 561, 566; dies ablehnend *Monka* in: BeckOK-StPO, § 136a StPO, Rn. 29; *Wolter* in: SK-StPO, § 136a StPO, Rn. 99, 105; *Wesemann/Müller*, StraFo 1998, 113; mit der Tendenz diese Problematik wohl zu Gunsten einer Disponibilität neu zu überdenken *Gless* in: LR-StPO, § 136a StPO, Rn. 71.
1291 BT-Drs. 15/4533, S. 15.

wenn man dem Angeklagten den Nachweis seiner möglichen Entlastung mit dem Verweis auf ein bestehendes Beweisverbot versagen würden.[1292] Korrekterweise muss dieser Begründungsansatz jedoch an einem tieferen Punkt ansetzen. Durch eine Zustimmung zur Verwertbarkeit würde der Betroffene auf den Schutz des Kernbereichs, der eine Ausprägung der allgemeinen Menschenwürde darstellt, verzichten. Somit muss die Frage geklärt werden, ob die Menschenwürde und damit auch der Kernbereich der Disposition des Betroffenen entzogen ist.[1293] Die Frage abstrakt beantwortend ist sich die herrschende Lehre und die höchstrichterliche Rechtsprechung einig, aus der „Unveräußerlichkeit" der Menschenwürde in Art. 1 Abs. 2 GG deren Unverzichtbarkeit zu folgern.[1294] So wurde in Urteilen zum Zwergenweitwurf,[1295] Peep-Shows[1296] und bei den Laserdrome-Fällen[1297] in der Menschenwürde ein objektiv unverzichtbarer Wert erblickt, auf welchen nicht verzichtet werden könne.[1298]

Gleichwohl ist zu sehen, dass der Strafprozess eine besondere Situation darstellt und der in diesem Zusammenhang erfolgte Grundrechtsverzicht nicht mit den übrigen Fällen zu vergleichen ist. Würde man dem Betroffenen die Möglichkeit des Grundrechtsverzichtes nehmen und ihm so seine womöglich letzte Möglichkeit seine Unschuld zu beweisen verwehren, so entzöge man ihn damit sein Recht, seine Freiheit aus Art. 2 Abs. 2 S. 2 GG, zu verteidigen.[1299] Insbesondere konkurriert im hiesigen Beispiel nicht ein beliebiges Recht mit der Menschenwürde, sondern diese steht im Konflikt mit sich selbst. Es würde einen unerklärlichen Widerspruch mit der durch den Kernbereich eigentlich zu schützenden Menschenwürde bedeuten, wenn sich die Einhaltung des Schuldprinzip, aufgrund der unterbliebenen Berücksichtigung eines entlastenden Beweises, zulasten des Angeklagten nicht im Urteil widerspiegeln würde. Das der Verzicht der Menschenwürde stets auch im Lichte der dadurch beförderten Interessen zu erblicken

1292 *Wohlers*, JR 2012, 389, 390 f.; *Jahn*, Gutachten dt. Juristentag, C1, C 113; FS-Strauda/*Roxin/Schäfer/Widmaier*, 435, 436 f.; *Erb*, GA 2017, 113, 126; *Bruns* in: KK-StPO, § 100d StPO, Rn. 40.

1293 Vgl. auch *Dautert*, Beweisverwertungsverbote und ihre Drittwirkung, S. 147; *Seifert*, Jura 2007, 99, 103; *Brandis*, Beweisverbote als Belastungsverbote, S. 288 ff.

1294 Vgl. BGH, NJW 1976, 1883, 1885; BVerwG, NJW 1982, 664, 665; *Hillgruber* in: BeckOK-GG, Art. 1 GG, Rn. 74; *Fischinger*, JuS 2008, 808, 811.

1295 VG Neustadt, NVwZ 1993, 98, 99.

1296 BVerwG, NJW 1982, 664, 665.

1297 BVerwG, Urt. v. 13.12.2006 – 6 C 17/06.

1298 BVerfGE 45, 187, 229.

1299 *Brandis*, Beweisverbote als Belastungsverbote, S. 289.

ist, zeigt sich darin, dass auch das BVerwG in seinem Urteil zu Laserdrome-Spielen ausführte, dass die aus der Menschenwürde „herzuleitende Wertordnung der Verfassung nicht im Rahmen eines Unterhaltungsspiels zur Disposition steht“[1300]. Von einem solchen mindergewichtigen Zweck wie der bloßen Belustigung kann im hiesigen Beispiel, in welchem zum Schutze der Menschenwürde auf diese verzichtet wird nicht gesprochen werden. Schließlich bewegt sich der Grundrechtsverzicht im Strafprozess im Spannungsfeld mit dem Erhalt anderer Grundrechte des Grundrechtsträgers.[1301] Zurecht weist *Amelung* darauf hin, dass es sich bei einem derartigen Verzicht um eine "*eingriffsmildernde Einwilligung*" handelt.[1302] Schließlich geht es in diesem Fall darum, staatlichen Zwang zu mildern indem der Verzichtende sich dafür entscheidet, ein Rechtsgut preiszugeben, um ein anderes – das ihm wertvoller erscheint als das Aufgeopferte – vor dem staatlichen Zugriff zu retten.[1303] Ebenso ist zu berücksichtigen, dass im Falle der Aufzeichnung von dem Kernbereich zugehöriger Informationen, der Kernbereich und damit die Menschenwürde durch diese Aufzeichnung bereits erstmalig durch den Staat missachtet wurde. Der Verzicht auf den Kernbereich und damit auf Menschenwürde im Prozess stellt daher lediglich eine hierauf folgende Reaktion dar. Ausschlaggebend für diese Situation war ein Verfahrensfehler oder ein nicht zu rechtfertigender Grundrechtseingriff, der nun in eine zweite Benachteiligung des Angeklagten umschlagen würde, wenn dem Angeklagten diese Entlastungsmöglichkeiten zum Schutz seiner Rechte oder der Unverzichtbarkeit der Menschenwürde verwehrt bliebe.

Ferner steht dies auch nicht im Widerspruch zum mit der Unverwertbarkeit kernbereichsrelevanter Informationen verfolgten Zweck. Während bei einem unter Verstoß gegen § 136a StPO gewonnen Beweismittel möglicherweise auch von dessen inhaltlicher Fehlerhaftigkeit ausgegangen werden könnte,[1304] fußt das aus einer Kernbereichsverletzung erwachsende Verwertungsverbot nicht auf einer Unbrauchbarkeit des Beweismittels, sondern soll tatsächlich einzig dem Schutz des Betroffenen dienen.[1305] Hiergegen spricht auch nicht, dass das abweichende Votum in der Ta-

1300 BVerwG, Urt. v. 13.12.2006 – 6 C 17/06, Rn. 25.
1301 *Brandis*, Beweisverbote als Belastungsverbote, S. 290.
1302 *Amelung*, NStZ 1982, 38, 39.
1303 *Amelung*, NStZ 1982, 38, 39.
1304 *Kudlich* in: MüKo-StPO, Einl., Rn. 452; *Joerden*, JuS 1993, 927; *Lesch*, GA 2000, 355, 369.
1305 *Ellbog*en, NStZ 2006, 179, 180 f.; vgl. auch *Greven* in: KK-StPO, vor § 94 StPO, Rn. 12.

gebuchentscheidung des BVerfG ausführte, dass die strikte Unverwertbarkeit des kernbereichsrelevanter Informationen auch dann gelte, wenn die Verwertung ausschließlich zugunsten des Betroffenen erfolgen soll.[1306] Schließlich grenzen die Richter diesen Maßstab bereits im nächsten Satz dahingehend ein, dass der Betroffene davor geschützt werden müsse, „in einem Strafverfahren gegen seinen Willen mit einem seinen innersten Persönlichkeitsbereich betreffenden Lebenssachverhalt konfrontiert zu werden".[1307] Sofern der Beschuldigte davon überzeugt ist, entsprechende Informationen würden zu seiner Entlastung beitragen, würde ihm sein Selbstbestimmungsrecht über seine Intimsphäre und sein eigenes Ich gerade nicht durch eine staatliche Erwägung entzogen, sondern durch den Beschuldigten selbstbestimmt preisgegeben. Will man diesem tatsächlich ein selbstbestimmtes Ich zugestehen, so ist es gerade die Pflicht des Rechtsstaates, dem Angeklagten diese Dispositionsmöglichkeit – in Anbetracht des dadurch verfolgten Zweckes – auch bei der Betroffenheit der Intimsphäre zu überlassen.[1308] Es ist daher richtig und notwendig die Verwertung eines Beweismittels als Entlastungsbeweis zugunsten des Betroffenen stets zuzulassen, während für die Verwertung als Belastungsbeweis die bekannten Grundsätze gelten.[1309] Hierfür streitet schlussendlich auch das pathosbehaftete, aber im Kern zutreffende Argument, dass es rechtsstaatlich unverantwortlich erscheinen würde, dass ein Gericht „sehenden Auges einen Unschuldigen oder weniger Schuldigen zum Opfer eines Fehlurteils machen muss"[1310].

2) Teilweise Verwertbarkeit des Beweismittels zur eigenen Entlastung

Unbeantwortet bleibt damit aber die Frage, ob diese Disponibilität dem Angeklagten auch dann zuzugestehen ist, wenn dieser nur eine Verwertung bestimmter Teile eines Beweismittels wünscht.[1311] Bei einer Audioaufzeichnung, die bspw. ein Selbstgespräch beinhaltet, würde der Angeklagte sodann nicht entscheiden, diese – als komplettes Beweismittel zu-

1306 So versteht wohl *Ladiges*, StV StV 2012, 517 f. jenes Urteil aus BVerfGE 80, 367, 382.
1307 BVerfGE 80, 367, 382 f.
1308 Vgl. auch *Brandis*, Beweisverbote als Belastungsverbote, S. 291.
1309 *Reinecke*, Fernwirkung von Beweisverwertungsverboten, S. 217 ff.; FS-Rehm/*Nack*, 310, 323.
1310 FS-Strauda/*Roxin/Schäfer/Widmaier*, 435, 441.
1311 Vgl. BGHSt 50, 206, 215; Habetha, ZWH 2012, 165, 166.

lassen zu wollen – sondern lediglich einzelne sekündlich oder minütlich begrenzte Abschnitte.

a) ablehnende Position

Die, die eine solche Aufspaltung ablehnen, begründen dies damit, dass man einen solchen der Rosinenpickerei ähnelnden Dispositionsgrundsatz – im Unterschied zum Zivilprozess – im Strafprozess nicht zulassen könne.[1312] Folglich kann der Angeklagte der Verwertung entweder ganz oder gar nicht zustimmen. Hierfür spreche auch, dass der Beweiswert eines solchen Beweismittels (das als solches ein dynamisches Gesamtgeschehen zeige) nur dann zuverlässig beurteilt werden kann, wenn dessen Inhalt dem Gericht in Gänze bekannt sei.[1313] Eine Teilung in verwertbare und nicht verwertbare Teile, scheitere sowohl an praktischen Schwierigkeiten als auch an der Ambivalenz von Detailaussagen.[1314] So könne der Trunkenheitsgrad bei Verkehrsdelikten im Lichte der §§ 20, 21 StGB einen entlastenden, im Rahmen der Straftaten aufgrund des alkoholisierten Fahrens gem. §§ 315c Abs. 1 Nr. 1a, 316 StGB wiederum einen belastenden Umstand darstellen.[1315]

b) Mühlenteichtheorie

Einen anderweitigen Ansatz, der zur Lösung dieses Problems fruchtbar gemacht werden kann, liefert die Mühlenteichtheorie[1316], die auf R*oxin, Schäfer* und *Widmaier* zurückgeht.[1317] Diese gehen im Grundsatz davon aus, dass ein Beweismittel soweit es Entlastendes enthält, zugunsten des Angeklagten berücksichtigt werden müsse.[1318] In der Praxis soll dies (hinsichtlich sämtlicher Fälle, die die mögliche Disponibilität eines Be-

1312 *Greven* in: KK-StPO, vor § 94 StPO, Rn. 12; *Nack,* StraFo 1998, 366, 371.
1313 *Greven* in: KK-StPO, vor § 94 StPO, Rn. 12; *Nack,* StraFo 1998, 366, 371.
1314 *Hamm*, NJW 1996, 2185, 2187.
1315 *Hamm*, NJW 1996, 2185, 2187.
1316 Der Name dieser Theorie geht nicht auf deren Inhalt, sondern auf den Ort eines Fortbildungslehrganges im ehemaligen „Kurhaus am Mühlenteich" zurück, vgl. Jahn, JuS 2008, 1122.
1317 *Roxin//Schäfer/Widmaier*, StV 2006, 655 ff.
1318 *Roxin//Schäfer/Widmaier*, StV 2006, 655, 658.

weisverbotes zum Gegenstand haben[1319]) derart umgesetzt werden, dass das Gericht nach Aufforderungen durch den Angeklagten, entsprechende Sequenzen zu verwerten, erst dann auf das (komplette) kontaminierte Beweismittel zurückgreifen wird, wenn es aufgrund der sonstigen Beweismittel bereits zur Überzeugung von der Täterschaft des Angeklagten gekommen ist.[1320] Um das Urteil rechtsstaatlich abzusichern und keine möglicherweise entlastenden oder schuldmindernden Umstände außenvorzulassen, soll das Gericht in einem solchen Fall aus der Urteilsberatung in die Verhandlung zurückkehren und über das kontaminierte Beweismittel noch Beweis erheben.[1321]

c) Stellungnahme

Zuzugeben ist den Kritikern einer Aufspaltung eines Beweismittels, dass dadurch zu befürchten ist, dass sich der Angeklagte tatsächlich einzelne Gesprächsinhalte herausziehen könnte, die für sich betrachtet entlastend wirken, im Gesamtkontext der Audioaufzeichnung wiederum eine andere Deutung erzeugen würden. Damit es schlussendlich nicht der Angeklagte ist, der das Gericht auf diesem Wege „hinters Licht führen kann", ist die Aufspaltung einer Audioaufzeichnung abzulehnen. Damit auch die möglicherweise entlastenden Sequenzen korrekt eingeordnet werden können, muss eine solche Audioaufzeichnung – sofern sie Einfluss in die endgültige Urteilsfindung finden soll – in ihrem Gesamtzusammenhang, mithin vollständig durch das Gericht zur Kenntnis genommen werden.[1322] Mit diesem Erfordernis geht wiederum das Problem einher, dass wenn der Inhalt einer – eigentlich unverwertbaren – Audioaufzeichnung durch das Gericht bereits während der eigentlichen Beweisaufnahme zur Kenntnis genommen würde, bei aller Objektivität und Professionalität eines Richters bezweifelt werden darf, ob dieser auch unterbewusst in der Lage wäre von dieser Audioaufzeichnung, die womöglich auch belastende Inhalte enthält, nur die Entlastenden Inhalte zu berücksichtigen und zu gewichten. Zugespitzt wird diese Problematik durch die mögliche Anwesenheit zweier Schöffen, denen dies gar ohne juristische Ausbildung zugemutet

1319 Für die Widerspruchslösung ist dies gleichbedeutend mit einer deutlich geringeren Relevanz, vgl. *Roxin*, NStZ 2007, 616, 618.
1320 *Roxin//Schäfer/Widmaier*, StV 2006, 655, 659.
1321 *Roxin//Schäfer/Widmaier*, StV 2006, 655, 659.
1322 Vgl. auch *Gössel* in: LR-StPO, Einl., Rn. 36.

würde. Um diesen „bösen Schein" zu vermeiden, darf auf ein kontaminiertes Beweismittel, welches der Beschuldigte nur zu Teilen der Beweisaufnahme zugänglich machen will, erst zugegriffen werden, nachdem das Gericht aufgrund der vorliegenden Beweise von der Täterschaft und Schuld des Angeklagten überzeugt ist. Sodann kann, die Einwilligung des Angeklagten vorausgesetzt, auf das kontaminierte Beweismaterial – jedoch wie ausgeführt nur in Gänze – zurückgegriffen werden. Sofern die Richter nach der Beweisaufnahme ohnehin zu keiner Strafbarkeit gelangen würden, wäre es bereits nicht mehr notwendig, dass der Angeklagte zu seiner Verteidigung Teile seiner Intimsphäre im Prozess offenbaren müsste.

3) Disponibilität eines Beweismittels bei mehreren Mitangeklagten

a) Reichweite eines Beweisverwertungsverbotes

Hinsichtlich der grundsätzlichen Reichweite eines Beweisverwertungsverbotes geht die ständige höchstrichterliche Rechtsprechung davon aus, dass ein Verwertungsverbot nur zugunsten des Angeklagten wirkt, in dessen Interesse es entstanden ist.[1323] Im Zusammenhang mit einer unterbliebenen Beschuldigtenbelehrung gem. § 136 Abs. 1 S. 2 StPO[1324] und einer unterlassenen Benachrichtigung des Verteidigers gem. § 168c Abs. 5 S. 1 StPO[1325] entschied der BGH, dass diese Fehler die Verwertung der gewonnen Informationen gegen Mitangeklagte nicht hindern, da die Vorschriften allein dem Schutz des betroffenen Beschuldigten dienen[1326].

Für die hiesige Fallkonstellationen fragt sich daher, ob unverwertbare, möglicherweise gar dem Kernbereich zugehörende, Audioaufzeichnungen gegen Mitangeklagte verwertbar sind. Hinsichtlich der Betroffenheit des Kernbereichs muss jedoch unabhängig von etwaigen Rechtskreisgedanken auch hinsichtlich aller Mitangeklagten von einer Unverwertbarkeit ausge-

---

1323 BGH, NStZ 1994, 595, 596; BGH, StV 2001, 545; BGH, NJW 2002, 1279, 1280; BayObLG, StV 1995, 237; *Nack*, StraFo 1998, 366, 373; a.A. *Dencker,* StV 1995, 232, 235; *Hamm*, NJW 1996, 2185, 2189.

1324 BGH, NJW 1994, 3364, 3366; BGH, NStZ-RR 2016, 377; ablehnend *Jäger*, JA 2017, 74, 76.

1325 BGHSt 53, 191, 194 ff., zustimmend *Dautert,* Beweisverwertungsverbote und ihre Drittwirkung, S. 206 f.; *von der Lippe*, Die Widerspruchslösung der Rechtsprechung, S. 190 ff.; kritisch *Gless*, NStZ 2010, 98, 99 f.; *Fezer*, NStZ 2009, 524, 525; *Kudlich*, JA 2009, 660, 662.

1326 BGH, NJW 1994, 3364, 3366; BGHSt 47, 233, 234.

gangen werden. Schließlich soll die dem Kernbereich anhaftende Unverwertbarkeit den Betroffenen gerade auch davor schützen, dass der Kernbereich seiner Lebensführung der Öffentlichkeit zugänglich gemacht wird. Dies würde allerdings geschehen, wenn entsprechende Audioaufzeichnungen zur Belastung eines Mitangeklagten, in den gegen diesen anhängigen Strafprozess eingeführt werden. Selbstverständlich ist originärer Zweck des § 100d Abs. 2 StPO die Verwertbarkeit solcher Informationen gegen den Betroffenen zu verhindern. Gleichwohl ergibt sich aus Sinn und Zweck des Kernbereiches und der staatlichen Verpflichtung, diesen umfassend zu schützen, dass die dem Kernbereich zuzuordnenden Informationen auch nicht gegen diverse Mitangeklagte verwertet werden können, da das damit einhergehende Abspielen der entsprechenden Audioaufzeichnung in einem öffentlichen Prozess den Sinn und Zweck des Kernbereichs ad absurdum führen würde und dessen Schutzgehalt unvollkommen wäre.

Entsprechend der höchstrichterlichen Rechtsprechung könnte aber im Fall eines nicht auf den Kernbereich zurückzuführenden Beweisverwertungsverbotes hinsichtlich möglicher Mitangeklagter ein anderes Ergebnis vorliegen. Danach könnte ein fehlerhaft erlangtes Beweismittel gegen den jeweils anderen Mitangeklagten verwertet werden (sog. Überkreuzverwertung).[1327] Dies zu Ende gedacht, könnte der bei zwei Mitangeklagten vorliegende Rechtsverstoß (beispielsweise in Form der Missachtung des Richtervorbehalts) gleichwohl jeweils zur Überführung des anderen oder der übrigen Mitangeklagten führen.[1328] Dass dies weder dem Rechtsgedanken des Richtervorbehalts noch dem Gesetzesvorbehalts entspräche, dürfte offensichtlich sein. Aus dem Sinn und Zweck des Richtervorbehalts, eine vorbeugende richterliche Kontrolle im Ermittlungsverfahren zu statuieren, folgt, dass nur dann von einem rechtmäßig erlangten Beweismittel gesprochen werden kann, wenn dieses die richterliche Kontrolle derart durchlaufen hat, als dass es erst nach einer vorherigen richterlichen Anordnung erlangt wurde. Ist dies erfolgt, muss jeder Angeklagte, die bei einer rechtmäßigen Maßnahme gegen einen Dritten erlangten Beweismittel gegen sich gelten lassen. Im umgekehrten Fall muss dem Betroffenen dann aber auch das Recht zustehen, nur solche Beweismittel gegen sich gelten lassen zu müssen, die unter Einhaltung der grundlegenden Verfahrensprinzipien erlangt wurden. Es ist nicht ersichtlich und würde darüber hinaus auch nicht einleuchten, dass der Gesetzgeber gewollt hat, dass

1327 Vgl. hierzu *Dencker,* StV 1995, 232, 235.

1328 Die Überkreuzverwertung daher ablehnend *Jäger*, JA 2017, 74, 76; *Gless/Wennekers,* JR 2009, 383, 385; *Jahn,* Gutachten dt. Juristentag, C1, C 115.

der Richtervorbehalt nur den unmittelbar vor der Maßnahme Betroffenen durch einen vorgelagerten Rechtsschutz schützen soll, sodann aber für den mittelbar Betroffenen diese Schutzvorrichtungen nicht gelten. Überdies hat der BGH wenigstens bei einer Verletzung des § 136a StPO anerkannt, dass ein hiergegen verstoßendes Geständnis eines Angeklagten auch gegen einen Mitangeklagten nicht verwertet werden darf, da dieser auch durch das Geständnis eines Mitangeklagten belastet werden kann.[1329] Ebenso ist es aber möglich, dass ein Mitangeklagter durch die bei einer ohne richterliche Anordnung erfolgte Überwachung eines anderen Angeklagten erlangten Beweise belastet werden kann. Insofern spricht vieles dafür, dass bei einem schweren Verfahrensfehler wie der fehlenden richterlichen Anordnung einer Überwachung oder auch dem gänzlichen Fehlen einer tatbestandlichen Ermächtigungsgrundlage auch gegenüber dem Mitangeklagten grundsätzlich ein Verwertungsverbot besteht.

b) Disponibilität zugunsten der Verwertbarkeit

Daneben kann es jedoch vorkommen, dass ein Angeklagter ein zugunsten eines oder aller Mitangeklagten bestehendes Verwertungsverbot für sich als günstig erachtet und daher dessen Verwertung ausdrücklich wünscht, während die übrigen Mitangeklagten hierin nicht einwilligen. In dieser Konstellation sind zwei Fallgestaltungen zu unterscheiden. Zum einen der Fall, in welchem der der Verwertung widersprechende Angeklagte in einem Selbstgespräch den Mitangeklagten entlastenden, sich selbst aber belastende Inhalte offenbart. Und zum anderen den Fall eines zum Kernbereich gehörenden Zwiegespräches zweier Angeklagten bezüglich dessen lediglich einer der Angeklagten eine Verwertung wünscht.

aa) Eingriff in die Rechtssphäre nur eines Angeklagten

Bereits 1964 hat der BGH hinsichtlich der Verwertbarkeit unrechtmäßig erlangter Beweise zugunsten eines Mitangeklagten Stellung genommen und angemerkt, dass die Verwertung von Beweismitteln, die durch einen rechtswidrigen Eingriff in die Sphäre eines Angeklagten gewonnen wurden, dann zulässig sei, wenn dies die einzige Möglichkeit darstelle, einen Mitangeklagten von besonders schweren Anklagevorwürfen zu ent-

1329 *Dallinger* nach BGH, MDR 1971, 18.

lasten.[1330] In Fällen, die weniger starke Beschuldigungen zum Gegenstand haben, sei dies aufgrund des überwiegenden Persönlichkeitsrechts des durch die unrechtmäßige Beweiserhebung Betroffenen nicht möglich.[1331] Insofern sieht es der BGH folglich als entscheidendes Merkmal an, wie stark die dem Mitangeklagten zur Last gelegten Straftaten ausfallen.

Der Annahme,[1332] dass ein Beweisverwertungsverbot zugunsten eines Betroffenen, nicht verhindere, dass der Mitangeklagte diese Informationen zu seinen Gunsten nutzen könne, ist jedoch nur bedingt zu folgen. Aus dem Wesen eines Beweisverwertungsverbotes als Recht des Betroffenen, folge naturgemäß, dass jemand, der nicht Inhaber des Rechtes ist, aus diesem keine Ansprüche herleiten kann. Dies bedeutet, dass ein Mitgeklagter zu seinem eigenen Schutz nicht verlangen kann, dass sich ein anderer Mitangeklagter auf ein für ihn bestehendes Beweisverwertungsverbot i.S.d. Widerspruchslösung beruft.[1333] Andererseits folge daraus aber, dass ein Angeklagter nicht daran gehindert sei, die zum Schutze eines anderen Mitangeklagten kontaminierten Beweismittel zu seinen – des Angeklagten – Gunsten in das Verfahren einführen zu lassen.[1334] Insofern ist dieser Umkehrschluss jedoch inkonsequent. Wenn davon ausgegangen wird, dass der Rechteinhaber ausschließlich der tatsächlich Betroffene ist, leuchtet nicht ein, weshalb demjenigen der nicht Rechteinhaber ist, aus dieser ihm nicht zustehenden Rechtsposition das Recht zukommen soll, das durch den Betroffenen nicht freigegebene Beweismittel zu seinen Gunsten in den Prozess einzubeziehen. Für eine Verwertbarkeit entgegen der Einwilligung des Betroffenen kann – sofern dadurch der Kernbereich betroffen ist – auch nicht angeführt werden, dass auf Seiten des Mitangeklagten, der aus der Menschwürde abgeleitete Grundsatz der Wahrung des Schuldprinzips im Urteil streitet. Schließlich würde die Verwertung ebenfalls die Menschenwürde desjenigen verletzen, dessen dem Kernbereich zuzuordnendes Selbstgespräch hierzu im Prozess abgespielt werden müsste.[1335] Diese Kollision sich diametral gegenüberstehender, beiderseits aus der Menschenwürde abgeleiteter Prinzipien, lässt sich nicht im Sinne des

1330 BGHSt 19, 325, 332; a.A. *von der Lippe*, Die Widerspruchslösung der Rechtsprechung, S. 105.
1331 BGHSt 19, 325, 332 f.
1332 So *Güntge*, StV 2005, 403, 405.
1333 *Güntge*, StV 2005, 403, 404 f.
1334 *Güntge*, StV 2005, 403, 404 f. mit Ausnahme eines Verstoßes gegen § 136a Abs. 3 S. 2 StPO.
1335 *Wolter* in: SK-StPO, Einl., Rn. 255.

Mitbeschuldigten auflösen.[1336] Ansonsten hätte es dieser letztlich in der Hand über einen Kernbereichsverzicht des Betroffenen zu entscheiden. Willigt der Betroffene nicht in die Verwertung eines den Kernbereich betreffenden Beweismittels ein, so müssen sich auch übrige Mitbeschuldigte derart behandeln lassen, als sei dieses Beweismittel nicht existent. Unabhängig davon bleibt es dem Gericht vorbehalten, hieraus zugunsten eines Mitbeschuldigten entsprechende Schlüsse zu ziehen. Gleichsam verbietet es sich freilich aus der verweigerten Einwilligung zulasten des betroffenen Angeklagten negative Schlüsse zu ziehen.

Erst bei verfassungsrechtlich unterschiedlich stark gewichteten, zueinander in Kollision stehenden, Rechten, wenn also auf Seiten des Betroffenen zwar ein Beweisverwertungsverbot besteht, diesem jedoch nicht die absolute Schutzwürdigkeit des Kernbereichs zukommt, kann ein anderes Ergebnis gerechtfertigt sein. In diesen Fällen kann, um über die Verwendung des kontaminierten Beweismittels zu Entlastungszwecken zu entscheiden, die dem Mitangeklagten vorgeworfene Straftat berücksichtigt werden.[1337] Sind Beweismittel zulasten des Betroffenen nicht verwertbar, wird der Mitangeklagte jedenfalls bei Straftaten, bei denen eine Freiheitsstrafe und damit ein Eingriff in seine Freiheitsrechte zu erwarten ist, verlangen können, dass entsprechende, zugunsten des Betroffenen gesperrte Beweismittel, zu seinen Gunsten entlastend verwertet werden. Sein Recht, nicht wegen eines Sachverhaltes verurteilt zu werden, der den tatsächlichen Gegebenheiten nicht entspricht, wird sodann höher zu gewichten sein.[1338]

bb) Eingriff in die Rechtsphäre sämtlicher Mitangeklagter

Anders könnte sich dies darstellen, wenn die Maßnahme, durch welche das gesperrte Beweismittel hervorgebracht wurde, unmittelbar die Rechtssphäre sämtlicher Mitangeklagter beeinträchtigte. Fordert sodann ein Mitangeklagter unter Verzicht auf seinen Kernbereichsschutz die Verwertung eines Beweismittels, würde dies immer noch bedeuten, dass sodann die weiteren Betroffenen gezwungen wären, auf ihren Kernbereichsschutz ebenfalls zu verzichten. Gleichwohl ist in dieser Konstellation zu sehen,

1336 So auch *Traub*, Verwertbarkeit von Selbstgesprächen, S. 148 f.; *Dautert*, Beweisverwertungsverbote und ihre Drittwirkung, S. 153.

1337 Vgl. BGHSt 19, 325, 332 f.

1338 So auch *Meixner*, Das Widerspruchserfordernis, S. 245, jedoch ohne die Differenzierung in absolute und relative Beweisverwertungsverbote.

dass sämtliche sich in einem Gespräch befindlichen Personen damit rechnen müssen, dass die Beteiligten sensible Inhalte nicht geheim halten werden. Insofern wäre der betroffene Angeklagte auch nicht gehindert, über die besprochenen Inhalte vor Gericht frei zu sprechen. Darin, dass dieser Angeklagter zu seiner Entlastung darüberhinausgehend auf den Kernbereichsschutz verzichten möchte und die Verwertung eines kontaminierten Beweisstückes verlangt, verwirklicht sich lediglich das enttäuschte Vertrauen der übrigen Gesprächsteilnehmer in den Angeklagten, dem strafprozessual allerdings keine Bedeutung zukommt. Tatsächlich müssen dieses Risiko die übrigen Mitangeklagten tragen, die aus freien Stücken die entsprechende Unterredung mit dem betreffenden Angeklagten führten.[1339] Sofern ein Angeklagter folglich durch eine Maßnahme selbst betroffen ist, kann dieser ungeachtet eines entgegenstehen Willens der Mitangeklagten die Verwertung eines kontaminierten Beweismittels zu seiner Entlastung verlangen.[1340]

cc) Problematik einer gesplitteten Tatsachenfeststellung

Zu beachten ist, dass, selbst wenn ein Mitangeklagter die Verwertung zu seiner Entlastung verlangt, dies nichts an der Unverwertbarkeit des Beweisgehalts zulasten der übrigen Mitangeklagten ändert. Aufgrund der Einführung in den Prozess zugunsten des dies verlangenden Angeklagten, würde dasselbe Urteil – differenziert nach den Angeklagten – dann allerdings unterschiedliche Tatsachenfeststellungen enthalten.[1341] Unter Verweis hierauf wird die Disponibilität über ein Beweismittel bei mehreren Angeklagten teilweise abgelehnt.[1342] Schließlich hat sich auch der BGH in einer älteren Entscheidung gegen eine solche Tatsachenalternativität ausgesprochen.[1343] Es widerspreche dem in § 261 StPO verankerten Grundsatz der freien Beweiswürdigung, wenn das Gericht bei der Würdigung des Beweisergebnisses hinsichtlich eines Mitangeklagten einen Teil des zulässig eingeführten Verfahrensstoffes außer Betracht lassen müsse. Wegen des engen inneren Zusammenhangs der festzustellenden Vorgänge sei

1339 *Bruns* in: KK-StPO, § 100d StPO, Rn. 42.
1340 So auch *Amelung*, StraFo 1999, 181, 184, mit der Einschränkung das Beweismittel nur zugunsten des Freigabewilligen zu berücksichtigen.
1341 *Güntge*, StV 2005, 403, 404.
1342 *Schwaben*, Die personelle Reichweite von Beweisverwertungsverboten, S. 167.
1343 BGHSt 22, 372, 374.

nur eine einheitliche Tatsachenfeststellung hinsichtlich aller Angeklagten denkbar.[1344] Gerade wenn die beweisgegenständliche Audioaufzeichnung eine Interaktion zwischen den Angeklagten dokumentiere, könne diese – eben auch hinsichtlich des die Verwertung fordernden Angeklagten – nur dann sinnvoll gewürdigt werden, wenn das Verhalten aller Beteiligten an der Interaktion berücksichtigt wird.[1345] Andere sehen in der möglichen Konsequenz unterschiedlicher Tatsachenfeststellungen und -bewertungen ein Umstand der eben hinzunehmen sei.[1346] So seien differierende Sachverhaltsfeststellungen und -bewertungen dem Strafrecht – man denke an das Prinzip der Wahlfeststellung – nicht fremd.[1347] Dem widerspreche auch nicht das zitierte BGH-Urteil. Schließlich hatte dieses die Frage zum Gegenstand, ob bereits eine gesetzlich bestehende Beweiserhebungsmöglichkeit aufgrund des Interesses eines Mitangeklagten durch diese Beweiserhebung nicht belastet zu werden, eingeschränkt werden könne.[1348] Hier steht jedoch ein bereits bestehendes Beweisverwertungsverbot im Zentrum, das, ohne seine Wirkung für den begünstigten Angeklagten zu verlieren, als Entlastungsbeweis für einen Mitangeklagten dienen soll.[1349] Im Ergebnis ist das Verlangen nach einer möglichst für alle Angeklagten einheitlichen Tatsachengrundlage – sofern nach dem zuvor gesagten eine Disponibilität über ein Beweisverwertungsverbot bei mehreren Angeklagten möglich ist – nicht in der Lage, die Verurteilung eines eigentlich freizusprechenden Beschuldigten zu legitimieren.[1350]

4) Zwischenergebnis

Während die Widerspruchslösung in vielen Fällen unselbstständiger relativer Beweisverwertungsverbote dem Betroffenen die Disponibilität über ein Beweisverbot ermöglicht, muss dies dem Betroffenen Angeklagten auch in Fällen möglich bleiben, in denen ein absolutes Beweisverwertungsverbot die Verwertung grundsätzlich hindern würde. Es verbleibt in sämtlichen Fällen in den Händen des Betroffenen darüber zu entscheiden, ob er

1344 BGHSt 22, 372, 374; *Schwaben*, Die personelle Reichweite von Beweisverwertungsverboten, S. 167.
1345 *Bruns* in: KK-StPO, § 100d StPO, Rn. 42.
1346 *Güntge*, StV 2005, 403, 405; *Amelung*, StraFo 1999, 181, 185.
1347 *Güntge*, StV 2005, 403, 405.
1348 *Güntge*, StV 2005, 403, 405.
1349 *Güntge*, StV 2005, 403, 405.
1350 *Wolter* in: SK-StPO, Einl., Rn. 256; *Weßlau*, StV 2010, 41, 44.

ein kontaminiertes Beweismittel zur Entlastungszwecken im Prozess der Verwertung freigeben möchte. Nicht möglich ist für den betroffenen Angeklagten dagegen aus einem einheitlichen, für die Verwertung gesperrten, Beweismittel nur einzelne Teile für die Verwertung zuzulassen. Er kann nicht die für ihn vorteilhaften Sequenzen einer Audioaufzeichnung in den Prozess einführen, während das Abspielen der Aufzeichnung bei ihn möglicherweise belastenden Abschnitten gestoppt werden soll. Bei einem solchen, für den Angeklagten teilweise vorteilhaften Beweismittel, kann dieser jedoch – sofern das Gericht auf Grundlage der übrigen Beweismittel – zu einer Verurteilung kommen würde, die entsprechende Audioaufzeichnung vollumfänglich einer nachträglich Beweiswürdigung zuführen lassen. Sodann obliegt es dem Gericht, inwiefern der darin enthaltene Inhalt die Auffassung des Gerichts in eine strafmildernde oder strafschärfende Richtung beeinflusst. Will ein Angeklagter in einem Prozess mit mehreren Mitangeklagten auf ein Beweisverwertungsverbot verzichten, so ist zuvörderst zu fragen, zum Schutz wessen Rechte das Beweismittel dem Prozess entzogen ist sowie welches Gewicht dem die Sperrung begründenden Recht zukommt. Fordert ein Angeklagter ein kontaminiertes Beweismittel, das aufgrund eines Eingriffs in die Rechtssphäre eines Mitangeklagten gesperrt ist, zu seiner Entlastung in den Prozess einzuführen, ist dies – kein Einverständnis durch den Betroffenen vorausgesetzt – nur möglich, wenn erstens das Beweisverwertungsverbot nicht zum Schutz des Kernbereichs der privaten Lebensführung des Betroffenen besteht und zweitens auf Seiten des die Verwertung fordernden Mitangeklagten ein berechtigtes Interesse in Form einer zu erwartenden Freiheitsstrafe vorliegt. Griff die rechtswidrige Maßnahme dagegen in die Rechtssphäre mehrerer Angeklagter ein, so kann jeder betroffene Angeklagte das kontaminierte Beweismittel zu Entlastungszwecken in den Prozess einführen. Dass dies möglicherweise mit einer gespaltenen Tatsachenfeststellung hinsichtlich desjenigen zu dessen Gunsten des Beweismittel verwertet werden soll und den übrigen Mitangeklagten, für deren strafrechtliche Beurteilung das Beweismittel weiterhin gesperrt bleibt, einhergeht, muss im Sinne einer möglichst umfassenden Wahrheitsermittlung hingenommen werden.

V) Fernwirkung

Analog zu den aus den bekannten Überwachungsmethoden herrührenden Informationen, können auch die aus einem Zugriff auf einen Sprachassistenten bzw. Smart Speaker in Form des Endgeräts entspringenden In-

formationen aufgrund einer Fernwirkung unverwertbar sein. Insofern ist dieses klassische strafprozessuale Problem auch im hiesigen Kontext von Relevanz.

1) Kernbereichsbetroffenheit

Es ist zu fragen, wie damit umzugehen ist, wenn die Strafverfolgungsbehörden durch das unverwertbare Beweismittel auf weitere Beweismittel stoßen. So, wenn beispielsweise der Betroffene in einem unverwertbaren (Selbst-)Gespräch den Leichenfundort offenbart. Es fragt sich dann, ob das hinsichtlich des Selbstgespräches bestehende Beweisverwertungsverbot eine sog. Fernwirkung entfaltet, die auch die Verwertung der Leiche und daran gefundener Spuren als Beweismittel verbietet. Die mit der Diskussion um das Anerkennen einer Fernwirkung einhergehende Problematik liegt darin, dass wenn sich die Unverwertbarkeit auf weitere Beweismittel erstreckt, das Prinzip der Wahrheitsermittlung und die Herstellung materieller Gerechtigkeit über das ohnehin bereits bestehende Beweisverwertungsverbot noch weiter eingeschränkt würde. Anderseits bestünde die Gefahr, dass das zum Schutze des Betroffenen entstandene Beweisverbot durch die Möglichkeit der Verwertung auf Grundlage des kontaminierten Beweismittels gefundener Beweise umgangen wird.[1351]

Jedenfalls dann, wenn ein aufgrund einer Kernbereichsbetroffenheit für den Prozess gesperrtes Beweismittel als Spurenansatz verwendet werden soll, ist sich Rechtsprechung und Literatur einig, dass sodann eine Fernwirkung besteht, die jegliche Verwendung des sekundär erlangten Beweismittels im weiteren Verfahren ausschließen muss.[1352] Der absolute Kernbereichsschutz wäre unvollständig, wenn zwar nicht das Selbstgespräch als solches, jedoch sämtliche aus diesem in der Folge womöglich generierten Beweise verwertbar wären. Zur Gewährleistung dieses Schutzes ist es, wie das BVerfG in der Entscheidung zum großen Lauschangriff feststellte, da-

1351 *Trüg*, Lösungskonvergenzen trotz Systemdivergenzen, S. 304.

1352 BVerfGE 109, 279, 331, *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, S. 69, 125; *Traub*, Verwertbarkeit von Selbstgesprächen, S. 151; *Eschelbach* in: SSW-StPO, § 100d StPO, Rn. 18; *Wolter* in: SK-StPO, § 100c StPO, Rn. 71; Großmann, JA 2019, 241, 246; *Gercke*, GA 2015, 339, 349; *Kretschmer*, HRRS 2010, 551, 552; *Ellbogen*, NStZ 2001, 460, 465; *Mitsch*, NJW 2012, 1486, 1488; hinsichtlich § 100c Abs. 5 S. 3 StPO a.F. vgl. BT-Drs. 15/4533, S. 15, wobei die Verweisung in BT-Drs 18/12785, S. 56 zeigt, dass diese Erwägung auch nach Einführung des § 100d Abs. 2 StPO gelten soll.

her erforderlich, dass aus einem dem Kernbereich zuzuordnenden Beweisstück herrührende Informationen „*insgesamt und ungeachtet ihres Inhalts im Strafverfahren nicht verwertet werden*".[1353] Insbesondere schließe dies auch aus, solche Informationen im weiteren Ermittlungsverfahren als Spurenansätze heranzuziehen.[1354]

2) Sonstige Fälle

Wesentlich umstrittener ist die Frage nach der Fernwirkung eines Beweisverbotes in sämtlichen übrigen Fällen.

a) Ablehnende Position

Allen voran die Rechtsprechung positionierte sich grundsätzlich gegen die Anerkennung einer Fernwirkung.[1355] So hat der BGH im Falle einer unzulässigen Telefonüberwachung nach § 100a StPO[1356] oder bei einem unter Verstoß gegen § 136a StPO erlangten Geständnis[1357] jegliche Fernwirkung abgelehnt. Hierfür sprächen vor allen Dingen Effektivitätsgedanken, da das Strafverfahren ansonsten durch jeden Verfahrensverstoß gelähmt würde.[1358] Ein weiteres Argument zur Begründung der Ablehnung der Fernwirkung sieht der BGH darin, dass sich kaum feststellen lasse, ob die Polizei das weitere Beweismittel nicht auch ohne den das primäre Beweismittel betreffenden Verstoß gefunden hätte.[1359] Einzig in einer Entscheidung aus dem Jahre 1980 nahm der BGH dagegen eine Fernwirkung an.[1360] In diesem Fall wurde wegen des Verdachts verfassungsfeindlicher Spionage, § 88 StGB und geheimdienstlicher Agententätigkeit, § 99 StGB eine Telefonüberwachung angeordnet, wobei sich schlussendlich allein eine Verletzung von Dienstgeheimnissen, § 353b StGB und Verwahrungsbruchs, § 133 StGB bewahrheitete. Da beide Taten keine Katalogtaten im Sinne des

1353 BVerfGE 109, 279, 331.
1354 BVerfGE 109, 279, 331.
1355 BGHSt 32, 68, 71; BGHSt 34, 362, 364; BGHSt 35, 32, 34; BGHSt 51, 1, 8; *BGH*, NStZ-RR 2016, 216; *Löffelmann*, JR 2019, 404, 405.
1356 BGHSt 32, 68, 71.
1357 BGHSt 34, 362, 364; kritisch *Seebode*, JR 1988, 427, 431.
1358 BGHSt 34, 362, 364; MüKo-StPO/*Peters*, § 152 StPO, Rn. 47.
1359 BGHSt 32, 68. 71.
1360 BGHSt 29, 244.

G 10 darstellten, war die durchgeführte Telefonüberwachung rechtswidrig. Unter Hervorhebung der hohen Bedeutung des Art. 10 GG und des Gesetzesvorbehalts kam der BGH unter teleologischen Gesichtspunkten zu dem Schluss, dass es für den grundrechtlichen Schutz des Betroffenen keinen Unterschied mache, ob die strafrechtliche Verfolgung aufgrund der unmittelbar durch die Telefonüberwachung oder nur der mittelbar erlangten Beweismittel erfolge.[1361] Gleichwohl war diese Entscheidung nicht in der Lage die höchstrichterliche Rechtsprechung nachhaltig zu ändern. Stattdessen wies der BGH in seinen späteren Urteilen ausdrücklich darauf hin, dass dieses Ergebnis allein für das in § 7 Abs. 3 G 10 a.F. normierte Verwertungsverbot gelten könne.[1362] Eine Begründung für diese Schlussfolgerung blieb der BGH jedoch stets schuldig. Dabei ist es vor dem Hintergrund durch die Verwertungsverbote die (Grund-)Rechte des Betroffenen zu wahren und ein faires Verfahren zu gewährleisten, in sämtlichen Fällen gleichgültig, ob der Betroffene unmittelbar durch die aus einer rechtswidrigen Maßnahme herrührenden Beweise oder „nur" mittelbar aufgrund der daraufhin erlangten Beweismittel einer strafrechtlicher Verfolgung ausgesetzt wird. Weshalb dies jedoch nach der Rechtsprechung des BGH nur im Lichte eines Verwertungsverbotes nach § 7 Abs. 3 G 10 a.F. der Fall sein soll, ist nicht zu erklären.

b) Befürwortende Position

Nach einer weit verbreiteten Literaturauffassung soll der amerikanischen fruit of the poisonous tree doctrin folgend, ein bestehendes Beweisverwertungsverbot stets mit einer Fernwirkung einhergehen.[1363] Zutreffend weist Fezer darauf hin, dass die Reichweite eines Verwertungsverbotes sich nicht an der Notwendigkeit eines Beweismittels für den Fortgang des Verfahrens orientieren könne, da ansonsten die gesamte Dogmatik der

1361 BGHSt 29, 244, 251.

1362 BGHSt 32, 68, 71; BGHSt 34, 362, 365.

1363 *Dencker*, Verwertungsverbote im Strafprozess, S. 76 ff.; *Koriath*, Beweisverbote im Strafprozess, S. 103; *Kühne*, Strafprozessrecht, Rn. 912.1; *Spendel*, NJW 1966, 1102, 1105; *Grünwald*, StV 1987, 470, 472 f.; *Otto*, GA 1970, 289, 293 f.; *Haffke*, GA 1973, 65, 82; *Riegel*, JZ 1980, 757; *Fezer*, JZ 1987, 936, 938; *Neuhaus*, NJW 1990, 1221, 1222; *Schroth*, JuS 1998, 969, 970; *Nüse*, JR 1966, 281, 284; *Benfer*, NVwZ 1999, 237, 239; *Klemke/Elbs*, Einführung in die Praxis der Strafverteidigung, Rn. 336; *Amelung*, NJW 1991, 2533, 2538; *Meyer-Mews*, HRRS 2015, 398, 405 f.; *Mende*, Grenzen privater Ermittlungen, S. 232 f.

Verwertungsverbote obsolet wäre.[1364] *Grünwald* erachtet eine solche strenge Regelung – überspitzt formuliert – als erforderlich, um zu verhindern, dass die Ermittlungsbehörden durch den unsachgemäßen Einsatz von Ermittlungsbefugnissen die Unverwertbarkeit des dadurch erlangten Beweismittels in Kauf nähmen, da schließlich weitere verwertbare mittelbare Beweismittel entstünden.[1365] Teilweise lassen Anhänger dieser Auffassung unter Heranziehung eines rechtmäßig alternativen Ermittlungsverlaufes die Verwertbarkeit, der aufgrund des kontaminierten und unverwertbaren Beweismittels dann zu, wenn die Strafverfolgungsbehörden diese Beweise ohnehin auch bei einem ordnungsgemäßen Verhalten entdeckt hätten.[1366]

c) Differenzierte Lösung

Andere wollen analog zur Begründung eines Beweisverwertungsverbotes auch das Bestehen einer Fernwirkung von einer Abwägung abhängig machen, in die wiederum auf der einen Seite die Schwere des zu dem Beweisverwertungsverbot führenden Rechtsverstoßes und auf der anderen Seite die Schwere der aufzuklärenden Straftat einzubeziehen ist.[1367] Gegen die generelle Annahme eines Beweisverwertungsverbotes nach amerikanischem Vorbild spreche, dass im dortigen Strafverfahren ein Beweisverwertungsverbot in erster Linie der Disziplinierung der Ermittlungsbeamten dienen, wohingegen dieser Zweck dem deutschen Strafverfahrensrecht fremd ist. Die vor diesem Hintergrund zu sehende Figur sei folglich nicht auf das deutsche Strafverfahrensrecht übertragbar.[1368]

1364 *Fezer*, JZ 1987, 937, 938.
1365 *Grünwald*, StV 1987, 470, 472 f.
1366 *Grünwald*, JZ 1966, 500; *Wolter*, NStZ 1984, 275, 277; *Amelung*, NJW 1991, 2533, 2539; *Schroth*, JuS 1998, 969, 970; *Beulke*, ZStW 1991, 657, 669, *Reinecke*, Fernwirkung von Beweisverwertungsverboten, S. 210 ff.
1367 MüKo-StPO/*Peters*, § 152 StPO, Rn. 48; *Schmitt* in: Meyer-Goßner/Schmitt, Einl. Rn. 57; *Bader* in: KK-*StPO*, Vor., § 48, Rn. 45 ff.; *Rogall*, NStZ 1988, 385, 392; *ders.*, ZStW 1979, 1, 39 f.; *Wolter*, NStZ 1984, 276, 277; *Maiwald*, JuS 1978, 379, 385; in diese Richtung auch BVerfG, NJW 2011, 2417, 2418, Rn. 42.
1368 *Schmitt* in: Meyer-Goßner/Schmitt, Einl, Rn. 57; FS-Beulke/*Ransiek*, 949, 949.

3) Stellungnahme

Unumstößlich ist, dass von Beweismitteln, die den Kernbereich oder die Intimsphäre des Betroffenen tangieren, grundsätzlich eine Fernwirkung ausgehen muss. In den übrigen Fällen verkennt das Argument, eine Fernwirkung führe zu einer Art der Verfahrenslähmung, dass es den Verfechtern einer Fernwirkung nicht darum geht, einen Verfahrensverstoß als Prozesshindernis zu behandeln, sondern um die Frage, ob Beweismaterial, das mittelbar auf Grund einer Verletzung von Verwertungsverboten erlangt wurde, verwertet werden darf.[1369] Vielmehr bleibt es selbstverständlich möglich, den Angeklagten mit Beweisen, die losgelöst vom Verstoß gegen die Rechte des Angeklagten erlangt wurden, zu überführen.[1370] Dagegen mutet es durchaus befremdlich an, wenn die Gerichte das vermeintliche Bedürfnis an solch makelbehafteten Beweisen mit der Notwendigkeit der Verhinderung einer Verfahrenslahmlegung begründen. Wenn die erst aufgrund der Rechtsverletzung aufgefundenen und daher mit diesem Verstoß bemakelten Beweise die einzigen sind, die die Verurteilung des Täters herbeiführen können, so stünde ein solches Verfahren auf wackeligen rechtsstaatlichen Beinen. In dem Fall, in dem ein solches Beweisstück eine Verurteilung wesentlich tragen würde, sollte noch viel mehr von dessen Unverwertbarkeit ausgegangen werden. Dass aber diejenigen, die in diesem Kontext erneut auf eine Abwägung zurückgreifen wollen, eine Fernwirkung zumeist gerade dann versagen, wenn dadurch ein entscheidendes Beweismittel betroffen ist, steht im Widerspruch zum Sinngehalt der Beweisverbote, der auch darin besteht, die Rechte des Betroffenen und die Rechtsstaatlichkeit des Strafverfahrens im Zweifel auch gegenüber kriminalpolitischen Zweckmäßigkeitserwägungen zu wahren.[1371]

Die oft bemühte Begründung, dass nicht jeder Verfahrensfehler das gesamte Strafverfahren lahmlegen dürfe,[1372] ist daher lediglich bei einem engen Verständnis dahingehend zutreffend, dass in der Tat nicht die bloße Entdeckung der Identität eines möglichen Verdächtigen durch einen rechtswidrig erlangten Beweis zu dessen Immunität gegen eine Strafverfol-

1369 *Grünwald*, StV 1987, 470, 472.
1370 *Roxin* in: Jauernig/Roxin, Die Rechtsprechung des BGH, S. 96 f.; *Klemke/Elbs*, Einführung in die Praxis der Strafverteidigung, Rn. 336.
1371 *Eisenberg*, Beweisrecht der StPO, Rn. 406.
1372 BGHSt 27, 355, 358; BGHSt 32, 68, 71.

gung führen darf, wenn die eigentlichen Beweismittel, die seine Schuld nachweisen, einwandfrei erlangt worden sind.[1373]

Insbesondere sprechen die gleichen Bedenken, die bereits hinsichtlich der Entstehung eines primären Beweisverwertungsverbotes durch die Heranziehung der Abwägungslehre geäußert wurden, auch dagegen die Erstreckung eines Beweisverwertungsverbotes in Form der Fernwirkung von solchen – rechtsunsicheren – Abwägungsentscheidungen abhängig zu machen.[1374] Zutreffend weist *Reinecke* darauf hin, dass jedenfalls der Umfang der Verwertbarkeit klar und eindeutig geregelt sein muss, wenn schon die vorangestellte Frage nach dem „Ob" einer Beweisverwertung höchst umstritten ist.[1375]

Demnach muss mit einer starken Literaturauffassung zunächst von einer Fernwirkung sämtlicher Beweisverwertungsverbote ausgegangen werden. Dem kann auch nicht mit dem Argument entgegnet werden, dass die dadurch herbeigeführte Disziplinierung der Strafverfolgungsbehörden dem deutschen Strafprozessrecht fremd ist. Denn tatsächlich steht ein solcher Disziplinierungsgedanken gar nicht im Zentrum dieser Betrachtungsweise, sondern vielmehr ein umfassender, nicht durch die Hintertür auszuhebelnder, Grundrechtsschutz. Dass womöglich dennoch ein Disziplinierungseffekt mit einer solchen Betrachtungsweise einhergeht, ist sodann ein bloßer Reflex, der aber nicht das eigentliche Ansinnen dieser restriktiven Sichtweise darstellt. Gleichwohl kann dieses Ergebnis keine ausnahmslose Geltung für sich beanspruchen. Analog zum Entstehen eines primären Beweisverwertungsverbots darf auch in diesem Zusammenhang dem Betroffenen kein ungerechtfertigter Vorteil in Form einer glücklichen Fügung zuteilwerden. Dies wäre dann der Fall, wenn das sekundäre Beweismittel mit an Sicherheit grenzender Wahrscheinlichkeit auch ohne das kontaminierte primäre Beweismittel erlangt worden wäre. Im Unterschied zur Anwendung der Figur des hypothetisch rechtmäßigen Ersatzeingriffes im Rahmen der Verwertbarkeit des primären Beweismittels ist Anhaltspunkt einer hypothetisch rechtmäßigen Beweismittelerlangung hier denklogisch nicht mehr das konkrete primäre Beweismittel (dieses ist, um überhaupt in die hiesige Situation zu gelangen, unverwertbar), sondern das mittelbare,

1373 *Harris*, StV 1991, 313, 320; vgl. *ders*. a.a.O. mit einer Analyse der Fernwirkung im amerikanischen Strafverfahren.

1374 *Jäger*, Beweisverwertung und Beweisverwertungsverbote, S. 116; *Reinecke*, Fernwirkung von Beweisverwertungsverboten, S. 232; *Eisenberg*, Beweisrecht der StPO, Rn. 408.

1375 *Reinecke*, Fernwirkung von Beweisverwertungsverboten, S. 232.

d.h. sekundär durch die rechtswidrige Beweisgewinnung erlangte Beweisstück. An dem zu fordernden restriktiven Hypothesenmaßstab vermag der unterschiedliche Bezugspunkt jedoch nichts zu ändern. Insbesondere bedeutet dies auch im hiesigen Kontext, dass nicht auf einer abstrakten Ebene die rechtswidrige Handlung durch eine theoretisch rechtmäßige Handlung ersetzbar ist, sondern das im konkreten Fall im Zeitpunkt der rechtswidrigen Erlangung des primären Beweismittels bereits ein zukünftiges Vorgehen im Ermittlungsverfahren angelegt war, das mit an Sicherheit grenzender Wahrscheinlichkeit ebenfalls zur Erlangung des mittelbaren, sekundären Beweismittels geführt hätte.

Die der Anwendung dieses Korrektiv zugrunde liegenden unterschiedlichen Bezugsunkte,[1376] werden im Falle der Beeinträchtigung des Kernbereichs oder der Intimsphäre auch im Ergebnis sichtbar. Während dieses Korrektiv, wenn es darum geht, eine ausnahmsweise Verwertbarkeit des primären Beweismittels zu begründen, im Falle der Kernbereichsbetroffenheit keine Anwendung finden kann, ist dies im Falle einer auf diesem Wege möglicherweise aufgehobenen Fernwirkung anders. Veranschaulicht werden kann dies am klassischen Lehrbuchfall[1377] zur Fernwirkung: Offenbart der Betroffene im Rahmen eines Selbstgespräches den Fundort der Leiche, so ist die Audioaufzeichnung des Gespräches freilich nicht verwertbar. Ebenso geht von diesem Beweisverbot eine Fernwirkung aus, die auch das Verwerten der Leiche als Beweismittel gegen den Betroffenen verbietet. War hingegen die Aushebung des betroffenen Erdreichs bereits nachweisbar geplant und insofern im Ermittlungsverfahren angelegt, wäre also die Leiche auch ohne die neuen Erkenntnisse aus dem Selbstgespräch später entdeckt worden, so ist der Leichnam als Beweismittel freilich verwertbar. Die von der kontaminierten Aufzeichnung des Selbstgespräches grundsätzlich ausgehende Fernwirkung kann das mittelbare Beweismittel folglich nicht gegen jegliche Verwertbarkeit im Strafprozess immunisieren.[1378]

1376 Zu nennen ist die Begründung der Verwertbarkeit eines primär rechtswidrig erlangten Beweismittel oder eine Ausnahme von einer bestehenden Fernwirkung hinsichtlich eines sekundären Beweismittels.

1377 Vgl. *Kudlich* in: MüKo-StPO, Einl., Rn. 488.

1378 Würde die Leiche gar ohne Kenntnis der Informationen aus dem Selbstgespräch, gewissermaßen zeitgleich mit dessen Aufzeichnung, ausgehoben, so wäre diese gar unproblematisch ohne Verknüpfung zur Problematik der Fernwirkung verwertbar.

4) Geltendmachung von Löschungsansprüchen

Um unabhängig von der Fernwirkung eine Konstellation zu verhindern, in welcher beispielsweise im Rahmen einer verdeckten Maßnahme Erkenntnisse erlangt wurden, aufgrund derer zu einem späteren Zeitpunkt eine an diese Erkenntnisse anknüpfenden Maßnahme durchgeführt werden könnte, ist es aus Sicht der Verteidigung ratsam, unmittelbar die dem Betroffenen zustehenden Löschungsansprüche geltend zu machen. Dies führt dazu, dass die Staatsanwaltschaft eine Einzelfallbearbeitung vorzunehmen hat, um dem konkreten Löschungsantrag des Betroffenen zu genügen.[1379] Auf die Löschung kann entweder im Dialog mit der Staatsanwaltschaft oder auf dem formalen Weg mittels gerichtlicher Überprüfung nach § 98 Abs. 2 S. 2 StPO bzw. im Wege der Beschwerde nach § 304 StPO hingewirkt werden.[1380]

Das BVerfG stützte diese Löschungspflicht ursprünglich auf § 489 StPO. Es führt aus, dass der Grundsatz der Verhältnismäßigkeit zwar bereits den staatlichen Zugriff auf Daten begrenzt, dies allein jedoch nicht genügt unzulässige Eingriffe in das Recht auf informationelle Selbstbestimmung zu verhindern. Vielmehr könne dies nur durch eine angemessene Verfahrensgestaltung erreicht werden.[1381] Auf das Volkzählungsurteil[1382] verweisend weist es darauf hin, dass gerade die Löschung aller nicht zur Zweckerreichung nicht erforderlichen Daten eine dieser verfahrensrechtlichen Schutzvorkehrungen darstellt.[1383] Über die strafprozessuale Vorschriften hinaus geben dem Betroffenen auch bereits die datenschutzrechtlichen Normen in Gestalt des § 75 Abs. 2 BDSG bzw. des hierzu korrespondierenden § 58 Abs. 2 BDSG ein Recht zur Datenlöschung, wenn die Verarbeitung der Daten unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist.[1384] Die Anwendung des BDSG auch im Bereich des Strafprozessrechts ergibt sich mittlerweile unproblematisch aus § 500 Abs. 1 StPO.[1385] Nur auf diesem Weg ist es möglich manifestierte

1379 OLG Dresden, MMR 2003, 592, 593.
1380 *Graßie/Hiéramente*, CB 2019, 191, 192.
1381 BVerfGE 113, 29, 57.
1382 BVerfGE 65, 1.
1383 BVerfGE 113, 29, 58.
1384 Vgl. *Basar/Hiéramente*, NStZ 2018, 681, 684.
1385 Vgl. BayObLG, ZD 2020, 359, das den Löschungsanspruch auf § 500 Abs. 1 StPO i.V.m. § 75 Abs. 2 BDSG, § 500 Abs. 2 Nr. 1 StPO i.V.m. § 489 Abs. 1 Nr. 1, Abs. 2 S. 3 StPO stützt, dabei jedoch darauf hinweist, dass eine Löschung

Erkenntnis aus Ermittlungsvorgängen endgültig aus der Ermittlungsakte zu verbannen. Besondere Bedeutung erlangt in diesem Zusammenhang der mit Wirkung für den 26.11.2019 eingeführte § 161 Abs. 2 S. 2 StPO, der § 58 Abs. 3 BDSG für unanwendbar erklärt. Das in § 58 Abs. 3 BDSG normierte Löschungssurrogat findet demnach keine Anwendung, wenn bereits die StPO eine Vorschrift für die Löschung personenbezogener Daten vorsieht. Dies ist in § 160a Abs. 1 S. 3 StPO, § 100e Abs. 6 Nr. 2 S. 3 StPO und § 101 Abs. 8 S. 1 StPO der Fall.[1386] Aus Sicht der Verteidigung führt dies zum erfreulichen Vorteil, dass die Strafverfolgungsbehörden den Betroffenen nicht lediglich mit dem Hinweis vertrösten können, die Verarbeitung der Daten einzuschränken, sondern diese unter den normierten Voraussetzungen tatsächlich unwiederbringlich zu löschen sind.

C. Nutzung der Daten zur Gefahrenabwehr

Nicht gesagt ist nach alle dem, dass die erlangten, aber letztlich im Strafprozess unverwertbaren Informationen, sofern darin entsprechende Anhaltspunkte vorkommen, nicht zu präventiven Zwecken, beispielsweise der Verhinderung einer geplanten Straftat genutzt werden dürfen.

I) Umwidmung repressiv erhobener Daten zu präventiven Zwecken

In der zweiten Tagebuchentscheidung des Bundesverfassungsgerichts kam die Bedeutung etwaiger Informationen für die präventive Sicherung Dritter und die Einschätzung der Gefahr weiterer Straftaten des Betroffenen bereits rudimentär zur Sprache.[1387] Die tragende Auffassung des Senats bejahte die Verwertbarkeit der Tagebuchaufzeichnungen unter anderem mit dem Argument, dass die Verwertung der Aufzeichnungen nicht nur der Ahndung der konkreten Straftat dienlich sei, sondern auch für die Einschätzung der Gefahr weiterer Straftaten des Beschwerdeführers wertvolle Hinweise liefere und insofern auch die Notwendigkeit einer präventiven

---

erst dann vorzunehmen ist, wenn das Ermittlungsverfahren erledigt ist, was regelmäßig erst bei einer Verfahrenseinstellung nach § 170 Abs. 2 StPO mit Eintritt der Verjährung gegeben sein wird.

1386 *Sackreuther* in: BeckOK-StPO, § 161 StPO, Rn. 15.

1387 BVerfGE 80, 367; *Wolter*, StV 1990, 175, 176.

Sicherung für das Überwiegen der Belange des Gemeinwohls spreche.[1388] Ungeklärt blieb damit allerdings die Frage, ob die Informationen zur präventiven Verwendung notwendigerweise überhaupt im Sinne eines repressiven Strafverfahrens verwertbar sein müssen.[1389]

Einfachgesetzlich ist an dieser Stelle § 479 Abs. 2 S. 2 Nr. 2 StPO näher zu betrachten. Während die Norm für eine gar rechtmäßige Beweiserlangung keine Anhaltspunkte enthält, ist ihrem Wortlaut dagegen an verschiedenen Stellen das Erfordernis verwertbarer Daten zu entnehmen. So erlaubt die Verwendungsbeschränkung in § 479 Abs. 2 S. 2 Nr. 2 StPO, dass *verwertbare* personenbezogene Daten, die durch eine Maßnahme erlangt worden sind, die nach der StPO nur bei Verdacht bestimmter Straftaten zulässig ist, „*zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für die Sicherheit oder den Bestand des Bundes oder eines Landes oder für bedeutende Vermögenswerte, wenn sich aus den Daten im Einzelfall jeweils konkrete Ansätze zur Abwehr einer solchen Gefahr erkennen lassen*“ verwendet werden dürfen. Für personenbezogene Daten aus den eingriffsintensiveren Maßnahmen nach § 100b StPO und § 100c StPO enthielt darüber hinaus § 479 Abs. 3 Nr. 1, 2 StPO a.F. eine speziellere Regelung. Durch das Gesetz zur Fortentwicklung der Strafprozessordnung und weiterer Vorschriften vom 25.06.2021 wurde § 479 Abs. 3 StPO a.F. jedoch wieder aufgehoben. Dem lag die Korrektur eines redaktionellen Versehens bei der Neufassung des § 479 StPO durch das Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 20.11.2019 zu Grunde.[1390] Ursprünglich sollte die Regelung des 479 Abs. 3 StPO a.F. die (besonderen) Verwendungsbeschränkungen aus § 100e Abs. 6 StPO für personenbezogene erlangte Daten aus Maßnahmen nach den §§ 100a, 100b StPO sowie die für § 100g Abs. 2 StPO geltenden (besonderen) Verwendungsbeschränkungen aus § 101a Abs. 4 StPO in § 479 Abs. 3 StPO zusammenfassen.[1391] Der Gesetzentwurf sah deshalb auch die Aufhebung der § 100e Abs. 6 StPO und des § 101a Abs. 4 StPO vor.[1392] Trotz der Neufassung des Abs. 3 in § 479 StPO wurden die entsprechenden – weitgehend inhaltsgleichen – Vorschriften der § 100e Abs. 6 StPO und § 101a Abs. 4 StPO jedoch nie aufgehoben. Nunmehr

1388 BVerfGE 80, 367, 380.
1389 Vgl. *Freiling/Safferling/Rückert*, JR 2018, 9, 15.
1390 *Wittig* in: BeckOK-StPO, § 479 StPO, Rn. 2.1.
1391 vgl. BT-Drs. 19/4671, S. 61, 65.
1392 vgl. BT-Drs. 19/4671, S. 8 f.

wurde stattdessen § 479 Abs. 3 StPO a.F. korrigierender Weise wieder aufgehoben, sodass hinsichtlich etwaiger Verwendungsbeschränkungen § 100e Abs. 6 StPO in den Blick zu nehmen ist.

Nach § 100e Abs. 6 Nr. 2 S. 1 StPO ist die Verwendung personenbezogenen Daten die durch Maßnahmen nach den §§ 100b und 100c StPO erlangt wurden nur „*zur Abwehr einer im Einzelfall bestehenden Lebensgefahr, einer dringenden Gefahr für Leib oder Freiheit einer Person oder für die Sicherheit oder den Bestand des Bundes oder eines Landes oder einer dringenden Gefahr für Gegenstände von bedeutendem Wert, die der Versorgung der Bevölkerung dienen, die von kulturell herausragendem Wert sind oder die in § 305 Absatz 1 des Strafgesetzbuches genannt sind*" zulässig. § 100e Abs. 6 Nr. 2 S. 2 StPO lässt darüber hinaus die Verwendung neben den in Satz 1 genannten Zwecken auch zur Abwehr einer im Einzelfall bestehenden dringenden Gefahr für sonstige bedeutende Vermögenswerte zu.

§ 100e Abs. 6 Nr. 2 StPO folgte auf den im Zuge der Umsetzung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017 veralteten § 100d Abs. 5 StPO a.F.[1393] Während noch in § 100d Abs. 5 StPO a.F. die Voraussetzung der „*verwertbaren personenbezogenen Daten*" lediglich in § 100d Abs. 5 Nr. 1 und 3 StPO a.F. (Verwertbarkeit der Daten in anderen Strafverfahren und Umwidmung präventiv erlangter Daten zu repressiven Zwecken) normiert war, wurde dieser Passus in § 100e Abs. 6 StPO vor die Aufzählung der einzelnen tatbestandlichen Nummern gezogen und würde dadurch nun für sämtliche Anwendungsfälle des § 100e Abs. 6 StPO Geltung beanspruchen.[1394] So war noch hinsichtlich § 100d Abs. 5 Nr. 2 StPO a.F. anerkannt, dass mangels Normierung der Voraussetzung der „Verwertbarkeit" auch die Verwendung strafprozessual nicht verwertbarer Daten zur Gefahrenabwehr zulässig ist.[1395] Der Gesetzgeber begründete dies damals äußerst zurückhaltend damit, „dass die schwierigen Fragen der strafprozessualen Verwertbarkeit der Daten im Zeitpunkt der Notwendigkeit der Gefahrenabwehr oftmals kaum verlässlich beantwortet werden können".[1396] Dass der Gesetzgeber durch die Neufassung des § 100e Abs. 6 StPO von diesem Verständnis auch nicht abrücken wollte, wird an verschiedenen Stellen ersichtlich. Bereits der Telos einer Umwidmung repressiv erhobener Daten zu präventiven Zwecken der Gefahrenabwehr gemeinsam mit dem Sinn

1393 vgl. BT-Drs. 18/12785, S. 58.
1394 *Freiling/Safferling/Rückert*, JR 2018, 9, 15.
1395 *Günther* in: MüKo-StPO, § 100d StPO, Rn. 40.
1396 vgl. BT-Drs. 15/5486, S. 18.

eines Beweisverwertungsverbotes im repressiven Sinne, spricht für eine Verwendung auch unverwertbarer Daten. Die präventive Nutzung der Daten verfolgt einzig das Ziel noch nicht geschehenes Unrecht abzuwenden. Es geht mithin nicht um die Ahndung begangener Straftaten, sondern vielmehr um die Umsetzung staatlicher Schutzpflichten zum Schutz der Bürger.[1397] Im Unterschied zum Strafverfahren wird im Rahmen der Gefahrenabwehr aufgrund der erlangten Informationen keine Verurteilung des Täters verfolgt, sondern die Rechtsgüter möglicher Opfer präventiv geschützt. Somit führt die präventive Verwendung repressiv unverwertbarer Informationen, gerade nicht zu einem gleich intensivem Grundrechtseingriff verglichen mit dem einer strafrechtlichen Verurteilung. Es wäre daher in der Tat nur schwer nachvollziehbar unter Verweis auf unverwertbare Daten, selbst wenn diese den höchstpersönlichen Kernbereich betreffen, die nun einmal bekannten Informationen nicht zur Verhinderung einer bevorstehenden Straftat einzusetzen.[1398] Dass der Gesetzgeber für eine präventive Verwendung der Daten nach § 100e Abs. 6 Nr. 2 StPO „verwertbare" Daten fordert, muss vielmehr als bloßes Redaktionsversehen eingeordnet werden.[1399] Insbesondere geben auch die Gesetzgebungsunterlagen keinen Aufschluss darüber, wieso im neugefassten § 100e Abs. 6 StPO das Erfordernis verwertbarer Daten nicht – analog zu § 100d Abs. 5 Nr. 1 und 3 StPO a.F. – auf die Anwendungsfälle des 100e Abs. 6 Nr. 1 und 3 StPO beschränkt blieb. Insofern musste bereits aus § 100e Abs. 6 Nr. 2 StPO gefolgert werden, dass die Umwidmung repressiver Daten zur Gefahrenabwehr auch für solche gilt, die im Strafprozess nicht verwertbar wären.[1400] Die teilweise vertretene Auffassung wonach der strikte Kernbereichsschutz auch hinsichtlich der Prävention gelten müsse und entsprechende Informationen auch nicht zur Gefahrenabwehr verwendet werden dürfe, ist damit ebenso wenig haltbar.[1401] Erfahren die Behörden etwa wie jemand im Selbstgespräch einen Mordplan verrät, so müssen und werden die Behörden selbstverständlich Vorkehrungen treffen, um die

1397 *Würtenberger/Heckmann/Tanneberger*, Polizeirecht, § 6, Rn. 177.
1398 *Zeitler/Turnit*, Polizeirecht, Rn. 794.
1399 Als eine von drei möglichen Auslegungen diese Lösung auch bei *Freiling/Safferling/Rückert*, JR 2018, 9, 16.
1400 Zutreffend auch *Graf* in: BeckOK-StPO, § 100e StPO, Rn. 36; *Bruns* in: KK-StPO, § 100e StPO, Rn. 26 hinsichtlich § 100e Abs. 6 Nr. 2 S. 1 StPO.
1401 Dem Willen des Gesetzgebers folgend, sollen solche Daten, die zur präventiven Gefahrenabwehr von Nöten sind, bereits nicht zum Kernbereich zu zählen sein, vgl. BT-Drs. 15/5486, S. 18; a.A. *Ellbogen*, NStZ 2001, 460, 463, *ders*. NStZ 2006, 180.

Tat zu verhindern.[1402] Im Übrigen sagt auch die zitierte Passage der Tagebuchentscheidung nichts über die Voraussetzung einer Umwidmung aus. Mit der Frage, inwiefern auf repressiver Grundlage rechtswidrig erlangte Daten, losgelöst von der Frage einer repressiven Verwertung, wenigstens zur Gefahrenabwehr genutzt werden dürfen, setzt sich das Urteil gerade nicht auseinander.[1403]

Im Übrigen werden in § 100e Abs. 6 StPO die Vorgaben, die das BVerfG in seiner Entscheidung zum großen Lauschangriff hinsichtlich dem Umgang mit repressiv gewonnenen Daten zur Gefahrenabwehr aufstellte, beachtet.[1404] Im Sinne der Einheit der Rechtsordnung darf die Übermittlungsschwelle nicht unter diejenige absinken, die im Rahmen der Gefahrenabwehr für entsprechende Eingriffe in das entsprechende Grundrecht gilt.[1405] Im Fall einer Überwachung von Vorgängen innerhalb der Wohnung sind mithin die in Art. 13 Abs. 4 GG für den präventiven Primäreingriff getroffenen Maßgaben zu berücksichtigen.[1406] Insofern sind die von § 100e Abs. 6 Nr. 2 S. 1 StPO hinsichtlich der Gefahrenintensität der Schutzgüter aufgestellten Anforderungen vergleichbar mit den nach Art. 13 Abs. 4 GG bestehenden Voraussetzungen für eine präventiv-polizeiliche Wohnraumüberwachung. Mit den Tatbestandsmerkmalen "Abwehr" und "im Einzelfall" verdeutlicht § 100e Abs. 6 Nr. 2 S. 1 StPO, dass eine Übermittlung nur bei konkreten Gefahren im polizeirechtlichen Sinne erfolgen darf.[1407] Auch durch den Verweis auf die Tatbestandsmerkmale Leben, Leib oder Freiheit benennt § 100e Abs. 6 Nr. 2 S. 1 StPO Gefahren für Rechtsgüter, die hinreichend bedeutsam sind, um den Einsatz technischer Mittel zur Überwachung von Wohnungen nach Art. 13 Abs. 4 GG zu legitimieren.[1408] Auch soweit eine Gefahr für erhebliche Sach- und Vermögenswerte genügen soll, ist in den im Rahmen der abschließenden Aufzählung genannten Fällen (Gegenstände von bedeutendem Wert, die der Versorgung der Bevölkerung dienen, die von kulturell herausragendem Wert sind oder die in § 305 Absatz 1 des Strafgesetzbuches genannt sind) regelmäßig anzunehmen, dass die Vorgaben des Art. 13 Abs. 4 GG,

1402 FS-Wolter/*Roxin,* 1057, 1075.
1403 Vgl. BVerfGE 80, 367, 380.
1404 BVerfGE 109, 279, 378 f.
1405 BVerfGE 100, 313, 394; BVerfGE 109, 279, 378.
1406 BVerfGE 109, 279, 378.
1407 BVerfGE 109, 279, 379; vgl. hierzu auch GS-Lisken/*Kutscha/Roggan*, 25, 39 f.
1408 Vgl. BVerfGE 109, 279, 379.

hinsichtlich des für eine gemeine Gefahr typischen Gefahrenpotential, gegeben sein werden.[1409]

Ist hingegen § 479 Abs. 2 StPO einschlägig (beispielsweise bei einer Maßnahme nach § 100a StPO) dürfen zu den in § 479 Abs. 2 S. 2 StPO genannten Zwecken nur verwertbare personenbezogene Daten verwendet werden. Der vor der Neufassung diesbezüglich geltende § 477 Abs. 2 S. 3 StPO a.F. enthielt eine solche Verwendungsbeschränkung dagegen noch nicht.[1410] Angesichts der nach hiesigem Verständnis großzügigeren Auslegung der Regelung in § 100e Abs. 6 Nr. 2 StPO bei Informationen, die gar aus den eingriffsintensivsten Maßnahmen der StPO stammen, erscheint diese enge Regelung in § 479 Abs. 2 S. 2 StPO nicht vollumfänglich zutreffend. Wenn schon unverwertbare, nach §§ 100b, 100c StPO erlangte, Informationen unter bestimmten Voraussetzungen zur Gefahrenabwehr verwendet werden dürfen, bestehen keine sachgemäßen Gründe, weshalb dies sodann nicht auch bei weniger intensiven Eingriffsmaßnahmen gelten sollte. Daher sollte § 479 Abs. 2 S. 2 Nr. 2 StPO derart einer teleologischen Extension zugeführt werden, dass Informationen aus Straftaten zur Gefahrenabwehr jedenfalls dann verwendet werden dürfen, wenn dies auch unter den in § 100e Abs. 6 Nr. 2 StPO normierten strengen Voraussetzungen zulässig wäre.

Die Möglichkeit bereits erlangte Informationen wenigstens zur präventiven Verbrechensverhütung zu nutzen, darf freilich nicht dazu führen, dass der Bürger durch eine grenzenlose Überwachung zum gläsernen Bürger wird. Angesichts dessen, dass die Anordnung einer Überwachungsmaßnahme ohnehin bereits den Anordnungsvoraussetzungen der §§ 100a ff. StPO genügen muss und ferner eine mögliche Umwidmung der erlangten Daten zur Gefahrenabwehr nur unter den zusätzlichen Voraussetzungen der §§ 100e Abs. 6, 479 StPO in Betracht kommen kann, wird dies auch nicht zu befürchten sein. Diese gesetzlichen Voraussetzungen stellen sicher, dass repressiv erlangte Daten nur in absoluten Ausnahmefällen, wenn das tatenlose Zusehen der Strafverfolgungsbehörden unter Verhältnismäßigkeitsgesichtspunkten schlechterdings unerträglich wäre, zur präventiven Gefahrenabwehr genutzt werden dürfen.

1409 BVerfGE 109, 279, 379.
1410 *Wittig* in: BeckOK-StPO, § 479 StPO, Rn. 9.

II) Möglichkeiten der praktischen Umsetzung

Bleibt die Frage, wie das aus den erlangten Daten vernommene Wissen praktisch zur Vermeidung einer geplanten Straftat eingesetzt werden kann. Eine Möglichkeit könnte es darstellen, den vermeintlichen zukünftigen Täter mit den bekannten Informationen zu konfrontieren. Auch wenn die Daten nicht auf repressiver Ebene verwertbar sind, wird der Täter das Gefühl haben, im Zusammenhang mit einer möglichen Straftat der Polizei bekannt zu sein. Die Wahrscheinlichkeit, dass die Strafverfolgungsbehörden sodann auf andere Weise belastende Inhalte gegen seine Person ermitteln, könnte den Täter sodann Abstand von der geplanten Tat nehmen lassen. Für den Täter würde dadurch das subjektiv wahrgenommene Entdeckungsrisiko deutlich steigen.[1411] Zwar ist aus kriminologischer Sicht durchaus anerkannt, dass das Entdeckungsrisiko mitursächlich für das Abstandnehmen eines tatbereiten Täters von der geplanten Straftat sein kann. Allerdings sollen diese Zusammenhänge primär im Bereich der Bagatellkriminalität gelten.[1412] Ebenso ist zu bedenken, dass je nach Naturell eines potenziellen Tatverdächtigen, dieser sich selbst durch ein hohes Entdeckungsrisiko nicht von der geplanten Straftat abschrecken lassen wird. Ob diese Unsicherheit angesichts des eindeutigen Wissens einer geplanten Straftat hingenommen werden kann, ist fraglich. Stattdessen wird die Möglichkeit der Anordnung einer Maßregel der Besserung und Sicherung, §§ 62 ff. StGB oder ihre einstweilige Anordnung nach § 126a StPO vorgeschlagen.[1413] Vor dem Hintergrund, dass die Gefahrenabwehrmaßnahme für den Betroffenen keine Strafe darstellen darf, da dieser gerade in keinem formalisierten Strafverfahren zu einer solchen verurteilt wurde und die betreffenden Informationen hierzu auch nicht verwertbar sind, muss dabei jedoch strikt beachtet werden, dass die damit einhergehende Freiheitsentziehung nicht gleichwohl zu einer verkappten Freiheitsstrafe wird. Angesicht der auch mit einer Sicherungsmaßregel einhergehenden Freiheitsentziehung, obgleich noch keine hierfür erforderliche Anlasstat vorliegt, hat der zuständige Ermittlungsrichter an die Verhältnismäßigkeitsprüfung gem. § 62 StGB besonders hohe Anforderungen zu stellen. Daneben erschiene auch ein auf ausschließlich präventivpolizeiliche Vorschriften gestütztes Tätigwerden möglich. Gem. § 39 Abs. 1 Nr. 3 BPolG kann zur Gefahrenabwehr, insbesondere wenn dies unerlässlich ist, um die

1411 Vgl. *Bock*, Kriminologie, Rn. 882; *Neubacher*, Kriminologie, § 8, Rn. 11 f.
1412 *Villmow* in: NK-StGB, Vor. § 38 ff., Rn. 79.
1413 *Wolter*, StV 1990, 175, 180.

unmittelbar bevorstehende Begehung oder Fortsetzung einer Straftat von erheblicher Bedeutung für die Allgemeinheit zu verhindern, der potenzielle Täter in Sicherungsgewahrsam genommen werden. Dieser ist in zeitlicher Hinsicht gem. § 42 Abs. 1 BPolG auf maximal vier Tage begrenzt. Ohne gegen den potenziellen Täter vorzugehen, verbleibt schließlich die Möglichkeit besondere Schutzvorkehrungen für das potenzielle Opfer zu treffen.

D. Ergebnis

Während der Einzug smarter Assistenten in den Alltag der Bürger und die damit einhergehenden Möglichkeiten der Strafverfolgung im Bereich des Zugriffs während des Ermittlungsverfahrens vielfach neue, kaum erörterte Fragestellungen aufwirft, rücken im Rahmen der Verwertbarkeit bereits seit Jahrzehnten im Zentrum der Rechtsprechung und Literatur stehende Thematiken erneut in den Vordergrund: Der Umfang des jedenfalls bei repressiver Zielrichtung absolut unverwertbaren Kernbereichs, die Bestimmung eines unselbstständigen ungeschriebenen Beweisverwertungsverbotes, der Umgang mit rechtswidriger Beweisgewinnung durch Private, die Disponibilität eines Beweisverwertungsverbotes zu Entlastungszwecken oder die Fernwirkungsproblematik beschäftigen Rechtsprechung und Literatur seit mehreren Jahren ununterbrochen. Wie sich zeigte, tendiert die Rechtsprechung in sämtlichen dieser Fragestellungen stets zu einer Effektivierung der Strafverfolgung und zeigt sich in der Anerkennung eines Beweisverwertungsverbotes zurückhaltend. Führt man sich daneben zudem vor Augen, dass den Strafverfolgungsbehörden mit jedem technischen Fortschritt stets neue Möglichkeiten der Beweismittelgewinnung zur Verfügung stehen, ist dies nicht zuletzt deshalb durchaus kritisch zu sehen. Ohne zu verkennen, dass eine effektive Strafjustiz elementarer Bestandteil eines funktionierenden Rechtsstaates ist, wäre eine mutigere Zuordnung entsprechender Inhalte zum Kernbereich wünschenswert. Wo dies für das Selbstgespräch erfreulicherweise bereits durch den BGH geschehen ist, müsste dies, um dem Betroffenen tatsächlich das Recht zuzugestehen in sozialen Bezügen zu existieren, auch für qualifizierte Zwiegespräche mit einem beichtenden / reflektierenden Charakter gelten.[1414] Entgegen dem Bundesverfassungsgericht kann die Kernbereichszugehörigkeit nicht durch einen unmittelbaren oder mittelbaren Straftatenbezug pauschal verneint

1414 § 5, A., I), 1), d).

werden. Auch in Fällen, die keine Kernbereichsbetroffenheit zum Gegenstand haben, wäre es im Sinne rechtssicherer und vorhersehbarer Ergebnisse wünschenswert sich mit einer verbreiteten Literaturmeinung hinsichtlich der Entstehung eines unselbstständigen ungeschriebenen Beweisverwertungsverbotes auf den eigentlichen Schutzzweck der Norm zur Ermittlung eines Beweisverbotes zu beschränken. Insbesondere die überproportional starke Gewichtung des Kriteriums der Tatschwere im Rahmen der Abwägungsdoktrin führt in der Praxis – willkürliche Entscheidungen der Ermittlungsbehörden ausgenommen – stetig zu einer Verwertbarkeit der unter Verstoß gegen die Regeln der Beweiserhebung erlangten Informationen. Eine tatsächliche Abwägung nehmen folglich oftmals nicht einmal die Verfechter einer solchen Abwägungslösung vor. Bei Zugrundelegung einer schutzzweckbasierten Beantwortung der Verwertbarkeitsfrage, sollte die Figur des hypothetisch-rechtmäßigen Kausalverlaufs in engen Grenzen als Korrektiv zur Vermeidung einer ungerechtfertigten Bevorteilung des Beschuldigten lediglich dann zum Einsatz kommen, wenn die Strafverfolgungsbehörden im konkreten Fall – ohne das diese dadurch „in die Vergangenheit zurückversetzt" werden und es lediglich zu einem hypothetischen Austausch des fehlerhaften Kausalfaktors kommt – das Beweismittel auch auf einem alternativen, bereits im Ermittlungsverfahren angelegten, Weg mit an Sicherheit grenzender Wahrscheinlichkeit erlangt hätten. Unter den gleichen engen Voraussetzungen ist auch eine Ausnahme von der von einem unverwertbaren Beweismittel grundsätzlich ausgehenden Fernwirkung hinsichtlich mittelbarer Beweismittel möglich.[1415] Kritisch zu sehen ist abschließend auch, dass es den Strafverfolgungsbehörden mit der höchstrichterlichen Rechtsprechung erlaubt ist, sich von einer rechtswidrigen, gar strafrechtswidrigen Beweiserlangung durch Privatpersonen freizusprechen und dies keinen Einfluss auf die Verwertbarkeit des Beweismittels hat. Dabei setzt sich das im durch den Privaten begangenen Rechtsverstoß wurzelnde Unrecht im hoheitlichen Verwertungsakt fort und wird durch die Verwertung aufrechterhalten und manifestiert. Daher sollte neben den Ausnahmefällen eines Menschenwürdeverstoßes, einer bewussten Umgehung der Beweiserhebungsvorschriften durch den Einsatz Privater und den Fällen, in denen die Verwertung einen Eingriff in die Intimsphäre des Betroffenen begründen würde, auch für strafrechtswidrig erlangte Beweismittel ein abwägungsresistentes Beweisverbot gelten.[1416] Zuletzt muss dem Betroffenen stets die umfassende Verfügungsgewalt über

1415 Vgl. § 5, B., I), 3).
1416 Vgl. § 5, B., II), 4).

ein zu seinem Schutz bestehendes Beweisverwertungsverbot verbleiben. Dies gilt jedenfalls so lange der Betroffene ein einheitliches Beweismittel nicht durch das Herauspicken einzelner, sodann aus dem Zusammenhang gerissener Audiosequenzen, verwertet wissen möchte. Sind in einem Prozess mehrere Personen angeklagt, ist hinsichtlich der Disponibilität entscheidend, in die Rechte welches Angeklagten durch die rechtswidrige Beweisgewinnung in welcher Intensität eingegriffen wurde.[1417]

1417 Vgl. § 5, B., IV), 3).

§ 6 Ausblick und Zusammenfassung

Smarte Haushaltsgeräte sind bereits heute mit stark zunehmender Tendenz verbreitet. Von den technischen Möglichkeiten ausgehend, können diese zu einer weitgehenden Überwachung der Bürger eingesetzt werden. Wie gezeigt können die durch Smart Speaker sowie die mit ihnen verbundenen Sprachassistenten generierten Daten in bestimmten Fällen bereits unter der aktuellen Rechtsordnung zur Strafverfolgung eingesetzt werden. Um diese Technologien für die Strafverfolgung nützlich zu machen, ist folglich nicht zwangsläufig eine neue Ermächtigungsgrundlage erforderlich. Da es lediglich eine Frage der Zeit ist, bis die bereits im Juni 2019 entbrannte Diskussion um den staatlichen Zugriff auf Smart Speaker erneut in das Zentrum der politischen Diskussionen rücken wird, versucht diese Arbeit sodann zu berücksichtigende Streitpunkte bereits aufzugreifen und einer möglichen Lösung zuzuführen. Nach der hier vertretenen Auffassung muss bei Suche nach einem tauglichen Gesetzesvorbehalt zwar konstatiert werden, dass die Interaktion mit einem Smart Speaker nicht unter einen strafprozessualen Telekommunikationsbegriff wie er in § 100a StPO zu fordern ist, subsumiert werden kann und darüber hinaus auch § 100a Abs. 1 S. 3 StPO aufgrund der festgestellten Verfassungswidrigkeit nicht als Ermächtigungsgrundlage in Betracht kommt. Die Online-Durchsuchung nach § 100b StPO stellt hingegen unter rechtlichen Gesichtspunkten einen gangbaren Weg dar, auf Smart Speaker zuzugreifen. Einem solchen Vorgehen steht jedoch – jedenfalls im Falle „datenloser" Smart Speaker – die praktische Hürde gegenüber, dass mangels gespeicherter Datenbestände auf diesen Endgeräten kein abschöpfbareres Material vorhanden ist. Entgegen vereinzelten Literaturauffassungen, die sich bereits mit den rechtlichen Möglichkeiten rund um Smart Speaker beschäftigten, ist es zulässig das Endgerät derart zu manipulieren, dass es gem. § 100c StPO als Wanze der Strafverfolgungsbehörden genutzt werden kann. Jedenfalls bei Smart-Speakern auf denen selbst keine Datenbestände gespeichert sind, ist dabei keine Kollision mit dem IT-Grundrecht zu befürchten und § 100c StPO auch vor diesem Hintergrund als taugliche Ermächtigungsgrundlage nicht zu beanstanden. Anders kann sich dies dann darstellen, wenn ein Sprachassistent als Wanze fungieren soll, der unmittelbar in ein Smartphone integriert ist und auf welchem eine Vielzahl an anderweitigen privaten Datenbeständen gespeichert sind. Sodann wäre es umso

bedeutender, ob die Software zur Manipulation des Sprachassistenten derart konfiguriert ist, dass lediglich laufende Gespräche überwacht werden können; die ruhenden Daten jedoch unangetastet bleiben. Daneben stehen den Ermittlungsbehörden auch offenen Ermittlungsbefugnisse zur Verfügung, die es ihnen beispielsweise erlauben sich Kenntnis der Zugangsdaten zum Account des Betroffenen zu verschaffen, um dort gespeicherte Daten zu sichten, § 110 Abs. 3 StPO, und gegebenenfalls beschlagnahmen zu können, § 94 StPO. Neben der Durchsuchung des Accounts über den Zugang des Betroffenen, kommt auch eine Durchsuchung des Serveraccounts beim Dienstleistungsanbieter in Betracht, die sich jedenfalls bei einer Kooperationsbereitschaft des Dienstleistungsanbieters ebenfalls nach § 102 StPO richten kann. Gleichwohl vergegenwärtigt die in dieser Arbeit enthaltene Diskussion um mögliche Ermächtigungsgrundlagen einschließlich der hierzu bestehenden unterschiedlichen Auslegungsmöglichkeiten eine de lege lata nicht gänzlich zu negierende Rechtsunsicherheit. Ob eine (extensive) Auslegung strafprozessualer Normen vor dem Hintergrund des damit zusammenhängenden Strafprozesses als des Rechtsstaates schärfstes Schwert im Sinne der Rechtssicherheit erstrebenswert ist, erscheint zumindest fraglich. Insofern könnte es angezeigt sein, dass sich der Gesetzgeber umfassend mit den zukünftig durch Smart-Home-Technologien im Allgemeinen aufkommenden rechtlichen Herausforderungen für das Strafverfahren auseinandersetzt und sodann möglicherweise eine exakt hierauf abgestimmte einheitliche Ermächtigungsgrundlage kodifiziert. Dies vor allem vor dem Hintergrund, dass die hier gegenständlichen Smart Speaker nur einen Teil der sprach- oder gestengesteuerten Smart-Home-Technologien abbilden. Beispielswiese ist auch an via Gestensteuerung gesteuerte Geräte zu denken, anhand derer Aktivierung beispielsweise auf die Anwesenheit einer Person, zu einer bestimmten Uhrzeit, an einem bestimmten Ort geschlossen werden soll.

Neben der Frage nach den Zugriffsmöglichkeiten, dürfen die mit der Existenz von Smart Speakern und einem Zugriff auf hierüber generierte Daten wieder in den Fokus rückenden Streitpunkte im Rahmen der Verwertbarkeit nicht außer Acht gelassen werden. Allein der Umstand, dass in diesem Bereich viele Punkte seit Jahren in Rechtsprechung und Literatur umstritten sind, zeigt die Notwendigkeit einer fortlaufenden kritischen Würdigung, um die verwertbarkeitsfreundliche Haltung der Rechtsprechung nicht ohne Weiteres hinzunehmen. Abermals soll hier auf zwei zentrale Punkte des § 5 dieser Arbeit verdeutlichend hingewiesen werden: In einer zunehmend digitalisierten Welt, in der der Bürger mehr und mehr gläsern wirkt, erscheint es umso wichtiger, diesem eine Sphä-

re zuzugestehen, in der er ausschließlich für sich sein kann. Jedenfalls bei Selbstgesprächen muss das staatliche Strafverfolgungsinteresse dabei uneingeschränkt zurückstehen. Darüber hinaus kann eine Existenz in sozialen Bezügen nur dann möglich sein, wenn auch für qualifizierte Zwiegespräche mit einem beichtenden / reflektierenden Charakter eine strikte Zuordnung zum unverwertbaren Kernbereich erfolgt. Die Abwägungslösung ist zur Begründung eines unselbstständigen Beweisverwertungsverbotes trotz ihrer vermeintlichen Einzelfallgerechtigkeit kritisch zu sehen. In diese – überspitzt formuliert „Verwertbarkeitslösung" – sollten Schutzzweckgesichtspunkte einen erheblich größeren Einfluss erhalten, wenn schon von der Abwägungsdoktrin ein Abrücken nicht zu erwarten ist. Zu überdenken ist auch der Umgang mit durch Privatpersonen generierten Beweismitteln. Da gerade Dritte durch die fortschreitende Digitalisierung den Alltag der Bürger mehr und mehr prägen und möglicherweise gar informationstechnisch beherrschen, muss deren Verhalten auch im Hinblick auf die Verwertung solcher Informationen im Strafprozess klare, bestimmbare und rechtssichere Grenzen gegenüberstehen. Keine Lösung stellt es in diesem Zusammenhang dar, den Betroffenen auf seine alleinige Verantwortung in diesem Zusammenhang hinzuweisen und ihn gewissermaßen mittelbar aufzufordern sich der fortschreitenden Digitalisierung zu verwehren. Der Rekurs auf das durch das StGB als strafbar normierte Verhalten, kann eine deutliche Grenze darstellen anhand derer festzustellen ist, ob der durch den Privaten begangenen Rechtsverstoß derart gravierend ist, dass das in diesem Rechtsverstoß wurzelnde Unrecht nicht im hoheitlichen Verwertungsakt fortwirken darf. So sehr die effektive Strafverfolgung als gewichtiges Ziel zur Wahrung der Verfassung anzuerkennen ist, so sehr dürfen jedoch auch nicht die Rechte jedes Einzelnen (Straftäters) diesem scheinbar übergeordneten Ziel zum Opfer fallen. Es ist gerade dieser Spagat zwischen einer effektiven Strafverfolgung und der fraglichen Rechtfertigung des damit zusammenhängenden Eingriffs in die Grundrechte des Betroffenen, der die Rechtsprechung und Literatur auch in den kommenden Jahrzehnten permanent beschäftigen wird. Angesichts der stetig zunehmenden Möglichkeiten des Staates sich auch über vernetzte Geräte – wie Smart Speaker mitsamt den hiermit verknüpften Sprachassistenten – Informationen zu beschaffen, ist eine kritische Auseinandersetzung mit der Verwertbarkeit solcher Informationen von umso größerer Bedeutung. Diesen Spagat (zu) einseitig zugunsten der effektiven Strafverfolgung zu lösen, mag rechtspolitisch zuweilen sinnvoll erscheinen, kann jedoch nicht über die rechtsdogmatischen Unbehaglichkeiten eines solchen Vorgehens hinweghelfen.

Literaturverzeichnis

Abraham Markus: Der Zugriff auf beim Provider gespeicherte E-Mails, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2021, S. 356 – 365, (zit.: *Abraham*, HRRS 2021, Seite)

Abraham, Markus: Hypothetischer Ersatzeingriff als Lauterkeitsargument, Zur Beweislast als Umgehungsschranke strafprozessualer Garantien, Zeitschrift für Internationale Strafrechtsdogmatik 2020, S. 120–132, (zit.: *Abraham*, ZIS 2020, Seite)

Albers, Marion: Informationelle Selbstbestimmung, Baden-Baden 2005, (zit.: *Albers*, informationelle Selbstbestimmung, Seite)

Albrecht, Florian / Braun, Frank: Die strafprozessuale Überwachung des Surfverhaltens, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2013, S. 500–508, (zit.: *Albrecht/Braun*, HRRS 2013, Seite)

Albrecht, Florian: Anm. zu OLG Köln 16. Zivilsenat, Beschluss vom 22.03.2013 – 16 Wx 16/12, jurisPR-ITR 14/2013 Anm. 4, (zit.: *Albrecht*, jurisPR-ITR 14/2013 Anm. 4)

Albrecht, Hans-Jörg / Dorsch, Claudia / Krüpe, Christiane: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen Abschlussbericht, Freiburg 2003, (zit.: *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation, Seite)

Allgayer, Peter: Strafprozessuale Unverwertbarkeit eines Selbstgesprächs im Auto, Neue Zeitschrift für Strafrecht 2012, S. 399–400, (zit.: *Allgayer*, NStZ 2012, Seite)

Amelung, Knut / Mittag, Matthias: Beweislastumkehr bei Haussuchungen ohne richterliche Anordnung gemäß § 105 StPO, Neue Zeitschrift für Strafrecht 2005, S. 614–617, (zit.: *Amelung/Mittag*, NStZ 2005, Seite)

Amelung, Knut: Die Verwertbarkeit rechtswidrig gewonnener Beweismittel zugunsten des Angeklagten und deren Grenzen, Strafverteidiger Forum 1999, S. 181–186, (zit.: *Amelung*, StraFo 1999, Seite)

Amelung, Knut: Die zweite Tagebuchentscheidung des BVerfG, Neue Juristische Wochenschrift 1990, S. 1753–1760, (zit.: *Amelung*, NJW 1990, Seite)

Amelung, Knut: Grundfragen der Verwertungsverbote bei beweissichernden Haussuchungen im Strafverfahren, Neue Juristische Wochenschrift 1991, S. 2533–2540, (zit.: *Amelung*, NJW 1991, Seite)

Amelung, Knut: Subjektive Rechte in der Lehre von den strafprozessualen Beweisverboten, Festschrift für Günter Bemmann zum 70. Geburtstag, S. 505–523, Baden-Baden 1997, (zit.: FS-Bemmann/*Amelung*, Seite)

Amelung, Knut: Verwendung eines Lügendetektors, Neue Zeitschrift für Strafrecht 1982, S. 38–40, (zit.: *Amelung*, NStZ 1982, Seite)

Amelung, Knut: Zur dogmatischen Einordnung strafprozessualer Grundrechtseingriffe, Juristenzeitung 1987, S. 737–745, (zit.: *Amelung*, JZ 1987, Seite)

Ametsbichler, Eva: Rechtliche Fragestellungen beim Einsatz von „Smart Home" – Technologie

Anders, Ralf Peter: Die Privatsphäre im Zeitalter von Big Data – Zum staatsanwaltschaftlichen Zugriff auf personenbezogene Daten in Speichern privater Dritter, Zeitschrift für Internationale Strafrechtsdogmatik 2020, S. 70–78, (zit.: *Anders*, ZIS 2020, Seite)

Angerer, Jörg: Kampf gegen Cybercrime – Phänomene und Ermittlungsprobleme, Deutsche Richterzeitung 2019, S. 428–431, (zit.: *Angerer*, DRiZ 2019, Seite)

Anke, Jürgen / Fischer, Uwe / Lemke, René: Integration digitaler Sprachassistenten in den Kundenservice am Beispiel der Stadtwerke Leipzig, Digitalisierung von Staat und Verwaltung, Gemeinsame Fachtagung Verwaltungsinformatik / Fachtagung Rechtsinformatik, S. 25–36, Münster 2019, (zit.: *Anke/Fischer/Lemke*, Digitalisierung von Staat und Verwaltung, Seite)

Arndt, Hans-Wolfgang / Fetzer, Thomas / Scherer, Joachim / Graulich, Kurt (Hrsg.): Telekommunikationsgesetz Berliner Kommentar, 2. Auflage, Berlin 2015, (zit.: *Bearbeiter* in: Arndt/Fetzer/Scherer/Graulich-TKG, § 3, Rn.)

Asbrock, Bernd: Gefahr im Verzug bei Durchsuchungen, Begründungsanforderungen an Durchsuchungsbeschluß, Strafverteidiger 2001, S. 322–324, (zit.: *Asbrock*, StV 2001, Seite)

Auer-Reinsdorff, Astrid / Conrad, Isabell (Hrsg.): Handbuch IT- und Datenschutzrecht, 3. Auflage, München 2019, (zit.: *Bearbeiter* in: Auer-Reinsdorff/Conrad, IT-R-HdB, §, Rn.)

Bachmaier, Werner: Dash-Cam & Co. – Beweismittel der ZPO?, Deutsches Autorrecht 2014, S. 15–22, (zit.: *Bachmaier*, DAR 2014, Seite)

Backes, Otto / Gusy, Christoph: Dokumentation – Wer kontrolliert die Telefonüberwachung? – Eine empirische Untersuchung von Richtervorbehalten bei Telefonüberwachungen, Strafverteidiger 2003, S. 249–252, (zit.: *Backes/Gusy*, StV 2003, Seite)

Backes, Otto / Gusy, Christoph: Wer kontrolliert die Telefonüberwachung?, Frankfurt 2003 (zit.: *Backes/Gusy*, Telefonüberwachung, Seite)

Bager, Jo / Zota, Volker: Smarte Alltagshelfer Alexa, Cortana, Google Assistant, Siri und Sony Assistant im Überblick, Magazin für Computertechnik 2016, Heft 26, S. 116 – 123, (zit.: *Bager/Zota*, c´t 2016, Heft, Seite)

Baldus, Manfred: Der Kernbereich privater Lebensgestaltung – absolut geschützt, aber abwägungsoffen, Juristenzeitung 2008, S. 218–227 (zit.: *Baldus*, JZ 2008, Seite)

Bantlin, Franziska: Grundrechtsschutz bei Telekommunikationsüberwachung und Online Durchsuchung, Juristische Schulung 2019, S. 669–673, (zit.: *Bantlin*, JuS 2019, Seite)

Bär, Wolfgang: Anm. zu LG Landshut, Beschluss vom 20.1.2011 – 4 Qs 346/10, Multimedia und Recht 2011, S. 691–693, (zit.: *Bär*, MMR 2011, Seite)

Bär, Wolfgang: Anmerkung zu LG Ellwangen, Beschluss vom 28.5.2013 – 1 Qs 130/12, Zeitschrift für Datenschutz 2014, S. 36–39, (zit.: *Bär*, ZD 2014, Seite)

Bär, Wolfgang: Der Zugriff auf Computerdaten im Strafverfahren, Würzburg 1992, (zit.: *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, Seite)

Bär, Wolfgang: Die Neuregelung des § 100j StPO zur Bestandsdatenauskunft – Auswirkungen auf die Praxis der Strafverfolgung, Multimedia und Recht 2013, S. 700–704, (zit.: *Bär*, MMR 2013, Seite)

Bär, Wolfgang: Strafprozessuale Fragen der EDV-Beweissicherung, Multimedia und Recht 1998, S. 577–584, (zit.: *Bär*, MMR 1998, Seite)

Bär, Wolfgang: Surfen im Internet als Teil der Telekommunikation i.S.d. § 100a StPO, Anmerkung zu BVerfG, Beschluss vom 6.7.2016 – 2 BvR 1454/13, Zeitschrift für Datenschutz 2017, S. 132–137, (zit.: *Bär*, ZD 2017, Seite)

Bär, Wolfgang: Transnationaler Zugriff auf Computerdaten, Zeitschrift für Internationale Strafrechtsdogmatik 2011, S. 53–59, (zit.: *Bär*, ZIS 2011, Seite)

Barczok, Achim: Amazon Echo: Mitarbeiter hören Audio-Mitschnitte ab, Magazin für Computertechnik 2019, Heft 10, S. 35, (zit.: *Barczok*, c´t 2019, Heft, Seite)

Barnitzke, Benno: Rechtliche Rahmenbedingungen des Cloud-Computing, Baden-Baden 2014, (zit.: *Barnitzke*, Rahmenbedingungen des Cloud-Computing, Seite)

Barrot, Johannes: Der Kernbereich privater Lebensgestaltung, Baden-Baden 2012, (zit.: *Barrot*, Der Kernbereich, Seite)

Basar, Eren / Hiéramente, Mayeul: Datenbeschlagnahme in Wirtschaftsstrafverfahren und die Frage der Datenlöschung, Neue Zeitschrift für Strafrecht 2018, S. 681–687, (zit.: *Basar/Hiéramente*, NStZ 2018, Seite)

Basar, Eren / Hiéramente, Mayeul: Datensparsamkeit in der StPO – Die Möglichkeit der Löschung, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2018, S. 336–342, (zit.: *Basar/Hiéramente*, HRRS 2018, Seite)

Battis, Ulrich:Schutz der Gewerberäume durch Art. 13 GG und Wirtschafts-, Arbeits- und Steueraufsicht, Juristische Schulung 1973, S. 25–30, (zit.: *Battis*, JuS 1973, Seite)

Bauer, Wolfram: Ist die Kritik an der "Rechtskreistheorie" (methodisch) noch zu halten?, Neue Zeitschrift für Strafrecht 1994, S. 2530–2531, (zit.: *Bauer*, NStZ 1994, Seite)

Bäumerich, Maik: Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung, Neue Juristische Wochenschrift 2017, S. 2718–2722, (zit.: *Bäumerich*, NJW 2017, Seite)

Baun, Christian / Kunze, Marcel / Nimis, Jens / Tai, Stefan: Cloud Computing – Web-basierte dynamische IT-Services, 2. Auflage, Berlin 2011, (zit.: *Braun/Kunze/Nimis/Tai*, Cloud Computing, Seite)

Becker, Christian / Meinicke, Dirk: Die sog. Quellen-TKÜ und die StPO – Von einer „herrschenden Meinung" und ihrer fragwürdigen Entstehung, Strafverteidiger 2011, S. 50–52, (zit.: *Becker/Meinicke*, StV 2011, Seite)

Becker, Florian: Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr, Neue Zeitschrift für Verwaltungsrecht 2015, S. 1335–1340, (zit.: *Becker*, NVwZ 2015, Seite)

Beck'scher Online Kommentar: Informations- und Medienrecht, Gersdorf, Hubertus / Paal, Boris (Hrsg.), 33. Edition, Stand: 01.05.2021, München 2021, (zit.: *Bearbeiter* in: BeckOK-InfoMedienR, Art., Rn.)

Beck'scher Online Kommentar: IT-Recht, Borges, Georg / Hilber, Marc (Hrsg.), 4. Edition, Stand: 01.10.2021, München 2021, (zit.: *Bearbeiter* in: BeckOK-ITR, Teil, §, Rn.)

Beck'scher Online Kommentar: Polizei- und Sicherheitsrecht Bayern, Möstl, Markus / Schwabenbauer, Thomas (Hrsg.), 16. Edition, Stand: 15.03.2021, München 2021, (zit.: *Bearbeiter* in: BeckOK-PolR Bayern, Art., Rn.)

Beck'scher Online-Kommentar: Gerichtsverfassungsgesetz, Graf, Jürgen-Peter (Hrsg.), 12. Edition, Stand: 15.08.2021 München 2021, (zit.: *Bearbeiter* in: BeckOK-GVG, §, Rn.)

Beck'scher Online-Kommentar: Grundgesetz, Epping, Volker / Hillgruber, Christian (Hrsg.), 48. Edition, Stand: 15.05.2021, München 2021, (zit.: *Bearbeiter* in: BeckOK-GG, Art., Rn.)

Beck'scher Online-Kommentar: Strafgesetzbuch, von Heintschel-Heinegg, Bernd (Hrsg.), 50. Edition, Stand: 01.05.2021, München 2021, (zit.: *Bearbeiter* in: BeckOK-StGB, §, Rn.)

Beck'scher Online-Kommentar: Strafprozessordnung mit RiStBV und MiStra, Graf, Jürgen-Peter (Hrsg.), 40. Edition, Stand: 01.07.2021, München 2021, (zit.: *Bearbeiter* in: BeckOK-StPO, §, Rn.)

Bedner, Mark: Cloud Computing – Technik, Sicherheit und rechtliche Gestaltung, Kassel 2012, (zit.: *Bedner*, Cloud Computing, Seite)

Behr, Johannes: Vollstreckung ohne Durchsuchungsanordnung, Art. 13 II GG, Neue Juristische Wochenschrift 1992, S. 2125–2128, (zit.: *Behr*, NJW 1992, Seite)

Bell, Anita: Beschlagnahme und Akteneinsicht bei elektronischen Medien, Hamburg 2016, (zit.: *Bell*, Beschlagnahme und Akteneinsicht, Seite)

Bell, Senta: Strafverfolgung und die Cloud, Berlin 2018, (zit.: *Bell*, Strafverfolgung und die Cloud, Seite)

Benfer, Jost: „Großer Lauschangriff" – einmal ganz anders gesehen, Neue Zeitschrift für Verwaltungsrecht 1999, S. 237–240, (zit.: *Benfer*, NVwZ 1999, Seite)

Bergemann, Nils: Die Telekommunikationsüberwachung nach der Entscheidung des Bundesverfassungsgerichts zum „großen Lauschangriff", Gedächtnisschrift für Hans Lisken, S. 69–86, Berlin 2004, (zit.: GS-Lisken/*Bergemann*, Seite)

Bergemann, Nils: Verdeckte Ermittlungen á la StPO: Ein unzureichender Regelungsversuch, Datenschutz und Datensicherheit 2007, S. 581- 585, (zit.: *Bergemann*, DuD 2007, Seite)

Berkemann, Jörg: Aus der Rechtsprechung des Bundesverfassungsgerichts, Juristische Rundschau 1990, S. 226–233, (zit.: *Berkemann*, JR 1990, Seite)

Bernsmann Klaus: Anm. zu BGH, Beschluss vom 21. 2. 2001 – 2 BGs 42/2001, Neue Zeitschrift für Strafrecht 2003, S. 103–104, (zit.: *Bernsmann*, NStZ 2003, Seite)

Bernsmann, Klaus / Jansen, Kirsten:Anm. zu LG Aachen, Beschluss v. 24.11.1998 – 64 Qs 78/98, Strafverteidiger 1999, S. 591–593, (zit.: *Bernsmann/Jansen*, StV 1999, Seite)

Beukelmann, Stephan: Online-Durchsuchung und Quellen-TKÜ, Neue Juristische Wochenschrift Spezial 2017, S. 440, (zit.: *Beukelmman*, NJW Spezial 2017, Seite)

Beulke, Werner / Meininghaus, Florian: Heimliche Online-Durchsuchung eines PC zugleich eine Anmerkung zu BGH, Beschluß vom 21.02.2006 – 3 BGs 31/06, Strafverteidiger 2007, S. 63–65, (zit.: *Beulke/Meininghaus*, StV 2007, Seite)

Beulke, Werner / Swoboda, Sabine:Strafprozessrecht, 15. Auflage, Heidelberg 2020, (zit.: *Beulke/Swoboda*, Strafprozessrecht, Rn.)

Beulke, Werner: Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus, Juristische Ausbildung 2008, S. 653–666, (zit.: *Beulke*, Jura 2008, Seite)

Beulke, Werner: Hypothetische Kausalverläufe im Strafverfahren bei rechtswidrigem Vorgehen von Ermittlungsorganen, Zeitschrift für gesamte Strafrechtswissenschaft 1991, S. 657–680, (zit.: *Beulke*, ZStW 1991, Seite)

Bierekoven, Christiane: Lizenzierung in der Cloud, Der IT-Rechts-Berater 2010, S. 42–44, (zit.: *Bierekoven*, ITRB 2010, Seite)

Birk, Dominik / Wegener, Christoph: Über den Wolken: Cloud Computing im Überblick, Datenschutz und Datensicherheit 2010, S. 641–645, (zit.: *Birk/Wegener*, DuD 2010, Seite)

BITKOM: Cloud Computing – Evolution in der Technik, Revolution im Business, BITKOM-Leitfaden Oktober 2009, Abrufbar: https://www.bitkom.org/sites/default/files/file/import/090921-BITKOM-Leitfaden-CloudComputing-Web.pdf, (zuletzt abgerufen am 31.10.2021) (zit.: *BITKOM*, Evolution in der Technik, Seite)

Blechschmitt, Lisa: Strafverfolgung im digitalen Zeitalter, MultiMedia und Recht 2018, S. 361–366, (zit.: *Blechschmitt*, MMR 2018, Seite)

Blechschmitt, Lisa: Zur Einführung von Quellen-TKU und Online-Durchsuchung, Strafverteidiger Forum 2017, S. 361–365, (zit.: *Blechschmitt*, StraFo 2017, Seite)

Bleich, Holger: Alexa, wer hat meine Daten?, Magazin für Computertechnik 2019, Heft 1, S. 16–18, (zit.: *Bleich*, c´t 2019, Heft, Seite)

Bludovsky, Oliver: Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100c Abs. 1 Nr. 3 StPO, Frankfurt 2002, (zit.: *Bludovsky*, Rechtliche Probleme beim Lauschangriff, Seite)

Bock, Michael: Kriminologie, 4. Auflage, München 2013, (zit.: *Bock*, Kriminologie, Rn.)

Bockemühl, Jan: Private Ermittlungen im Strafprozess, Baden-Baden 1996, (zit.: *Bockemühl*, Private Ermittlungen im Strafprozess, Seite)

Böckenförde, Thomas: Auf dem Weg zur elektronischen Privatsphäre, Juristenzeitung 2008, S. 925–939, (zit.: Böckenförde, JZ 2008, Seite)

Bode, Thomas: Verdeckte strafprozessuale Ermittlungsmaßnahmen, Heidelberg 2012, (zit.: *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, Seite)

Borges, Georg / Meents, Jan Gert: Cloud Computing Rechtshandbuch, München 2016, (zit.: *Bearbeiter* in: Borges/Meents Cloud-Computing, §, Rn.)

Böse, Martin: Die verfassungsrechtlichen Grundlagen des Satzes „Nemo tenetur se ipsum accusare", Goltdammers Archiv 2002, S. 98–128, (zit.: *Böse*, GA 2002, Seite)

Böse, Matthias / Rockenbach, Florian: Cloud Computing: Vertragliche und datenschutzrechtliche Besonderheiten in der Praxis, Monatsschrift für Deutsches Recht 2018, S. 70–74, (zit.: *Böse/Rockenbach*, MDR 2018, Seite)

Boss, Carina / Kroschwald, Steffen / Wicker, Magda: Datenschutz bei Cloud Computing zwischen TKG, TMG und BDSG – Datenkategorien bei der Nutzung von Cloud-Diensten, Zeitschrift für Datenschutz 2013, S. 205–209, (zit.: *Boos/Kroschwald/Wicker*, ZD 2013, Seite)

Brandis, Tobias: Beweisverbote als Belastungsverbote aus Sicht des Beschuldigten, Frankfurt 2001, (zit.: *Brandis*, Beweisverbote als Belastungsverbote, Seite)

Braun, Frank: Anmerkung zu: LG Ellwangen, Beschluss vom 28.05.2013 – 1 Qs 130/12, jurisPR-ITR 18/2013 Anm. 5 (zit.: *Braun*, jurisPR-ITR 18/2013 Anm. 5)

Bräutigam, Peter: IT-Outsourcing und Cloud-Computing, 4. Auflage, Berlin 2019, (zit.: *Bearbeiter* in: Bräutigam, IT-Outsourcing und Cloud-Computing, Teil, Rn.)

Brennscheidt, Kirstin: Cloud Computing und Datenschutz, Bochum 2013, (zit.: *Brennscheidt*, Cloud Computing und Datenschutz, Seite)

Brocker, Lars / Zartmann, Monika: Die verdeckte Datenerhebung aus Wohnungen zur Abwehr dringender Gefahren, Deutsche Richterzeitung 2005, S. 108–109, (zit.: *Brocker/Zartmann*, DRiZ 2005, Seite)

Brockmeyer, Henning / Vogt, Verena: Alexa, Siri & Google Assistant – was ist erlaubt? Sprachassistenten und das Recht, Phänomenen des Big-Data Zeitalters (Wissenschaftliche Schriften der WWU Münster, Reihe III, Band 35), S. 187–203, Münster 2019, (zit.: *Brockmeyer/Vogt*, Phänomenen des Big-Data Zeitalters, Seite)

Brodowski, Dominik / Eisenmenger, Florian: Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden – Sachliche und zeitliche Reichweite der „kleinen Online-Durchsuchung" nach § 110 Abs. 3 StPO, Zeitschrift für Datenschutz 2014, S. 119–126, (zit.: *Brodowski/Eisenmenger*, ZD 2014, Seite)

Brodowski, Dominik / Freilieng, Felix: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, Schriftenreihe Forschungsforum Öffentliche Sicherheit, Berlin 2011, (zit.: *Brodowski/Freiling*, Cyberkriminalität, Seite)

Brodowski, Dominik: Strafprozessualer Zugriff auf E-Mail-Kommunikation, Juristische Rundschau 2009, S. 402–412, (zit.: *Brodowski*, JR 2009, Seite)

Brookmann, Justin: Können wir der Cloud vertrauen?, Zeitschrift für Datenschutz 2012, S. 401–402, (zit.: *Brookmann*, ZD 2012, Seite)

Brunhöber, Beatrice: Privatisierung des Ermittlungsverfahrens im Strafprozess, Goltdammers Archiv 2010, S. 571–588, (zit.: *Brunhöber*, GA 2010, Seite)

Brüning, Janique: Der Richtervorbehalt – ein zahnloser Tiger?, Zeitschrift für Internationale Strafrechtsdogmatik 2006, S. 29–35, (zit.: *Brüning*, ZIS 2006, Seite)

Brüning, Janique: Der Richtervorbehalt im strafrechtlichen Ermittlungsverfahren, Baden-Baden 2005, (zit.: *Brüning*, Der Richtervorbehalt, Seite)

Brüning, Janique: Die Rechtsfolgen eines Verstoßes gegen den Richtervorbehalt, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2007, S. 250–255, (zit.: *Brüning*, HRRS 2007, Seite)

Brunst, Philip: Anm. zu BVerfG, Beschluss vom 16.6.2009 – 2 BvR 902/06, Computer und Recht 2009, S. 591–593, (zit.: *Brunst*, CR 2009, Seite)

Brunst, Philip: Staatlicher Zugang zur digitalen Identität, Datenschutz und Datensicherheit 2011, S. 618–623, (zit.: *Brunst*, DuD 2011, Seite)

Büddefeld, Dieter: Akustische Wohnraumüberwachung, Kriminalistik 2015, S. 204–207, (zit.: *Büddelfeld*, Kriminalistik 2015, Seite)

Buermeyer, Ulf: Die "Online-Durchsuchung". Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2007, S. 329–337, (zit.: *Buermeyer*, HRRS 2007, Seite)

Buermeyer, Ulf: Stellungnahme zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess Ausschuss-Drucksache 18(6)334, Berlin 2017, abrufbar unter: https://freiheitsrechte.org/home/wp-content/uploads/2017/05/Stellungnahme-RiLG-Dr.-Buermeyer-LL.M..pdf, (zuletzt abgerufen am 31.10.2021), (zit.: *Buermeyer*, Stellungnahme zur Ausschuss-Drucksache 18(6)334, Seite)

Buermeyer, Ulf: Zum Begriff der „laufenden Kommunikation" bei der Quellen-Telekommunikationsüberwachung, Strafverteidiger 2013, S. 470–476, (zit.: *Buermeyer*, StV 2013, Seite)

Bung, Jochen / Huber, Verena: Zur Drittwirkung von Grund- und Menschenrechten im Strafverfahren, Festschrift für Werner Beulke zum 70 Geburtstag, S. 655–669, Heidelberg 2015, (zit.: FS-Beulke/*Bung/Huber*, 655, 666)

Bung, Jochen: Grundlagenprobleme der Privatisierung von Sanktions- und Präventionsaufgaben, Zeitschrift für die gesamte Strafrechtswissenschaft 2013, S. 536–550, (zit.: *Bung*, ZStW 2013, Seite)

Bunzel, Maik: Der strafprozessuale Zugriff auf IT-Systeme, Berlin 2015, (zit.: *Bunzel*, Der strafprozessuale Zugriff auf IT-Systeme, Seite)

Burhoff, Detlef: Die Bestandsdatenauskunft, Strafrechtsreport 2015, S. 8–11, (zit.: *Burhoff*, StRR 2015, Seite)

Busching, Michael: Der Schutz privater Informationen bei Cloud Computing, Tübingen 2019, (zit.: *Busching*, Der Schutz privater Informationen bei Cloud Computing, Seite)

Ciolek-Krepold, Katja: Durchsuchung und Beschlagnahme im Wirtschaftsstrafverfahren, München 2000, (zit.: *Ciolek-Krepold*, Durchsuchung und Beschlagnahme im Wirtschaftsstrafverfahren, Seite)

Cornelius, Kai: Anm. zu BGH-Beschluss vom 31. Januar 2007, Juristenzeitung 2007, S. 798–800, (zit.: *Cornelius*, JZ 2007, Seite)

Cornelius, Kai: Cloud Computing für Berufsgeheimnisträger, Strafverteidiger 2016, S. 380–390, (zit.: *Cornelius*, StV 2016, Seite)

Cornelius, Kai: Verwertung privat gefertigter Dashcam-Videos im Verkehrs-Bußgeldverfahren, zugleich Anmerkung zu OLG Stuttgart, Beschluss vom 4.5.2016 – 4 Ss 543/15, Neue Juristische Wochenschrift 2016, S. 2282–2283, (zit.: *Cornelius*, NJW 2016, Seite)

Dalakouras, Theoharis: Beweisverbote bezüglich der Achtung der Intimsphäre, Berlin 1988, (zit.: *Dalakouras*, Beweisverbote und Intimsphäre, Seite)

Dalby, Jakob: Das neue Auskunftsverfahren nach § 113 TKG, Computer und Recht 2013, S. 361–369, (zit.: *Dalby*, CR 2013, Seite)

Dalby, Jakob: Grundlagen der Strafverfolgung im Internet, Münster 2015, (zit.: Dalby, Strafverfolgung im Internet, Seite)

Dallinger, Wilhelm: Aus der Rechtsprechung des Bundesgerichtshofs in Strafsachen, Monatsschrift für Deutsches Recht 1956, S. 143–146, (zit.: *Dallinger,* MDR 1956, Seite)

Dallinger, Wilhelm: Aus der Rechtsprechung des Bundesgerichtshofs in Strafsachen, Monatsschrift für Deutsches Recht 1971, S. 15–19, (zit.: *Dallinger*, MDR 1971, Seite)

Dallmeyer, Jens: Beweisführung im Strengbeweisverfahren, Frankfurt 2002, (zit.: *Dallmeyer,* Beweisführung im Strengbeweisverfahren, Seite)

Dammann, Ilmer: Der Kernbereich der privaten Lebensgestaltung, Berlin 2011, (zit.: *Dammann*, Der Kernbereich der privaten Lebensgestaltung, Seite)

Dautert, Franziska: Beweisverwertungsverbote und ihre Drittwirkung, Berlin 2014, (zit.: *Dautert*, Beweisverwertungsverbote und ihre Drittwirkung, Seite)

Deiters, Mark / Albrecht, Anna Helena: Anm. zu BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07 und 1 BvR 595/07, Zeitschrift für das Juristische Studium 2008, S. 319–324, (zit.: *Deiters/Albrecht*, ZJS 2008, Seite)

Delius, Gerhard: Tagebücher als Beweismittel im Strafverfahrensrecht, München 1967, (*Delius*, Tagebücher als Beweismittel, Seite)

Demko, Daniela: Die Erstellung von Bewegungsbildern mittels Mobiltelefon als neuartige strafprozessuale Observationsmaßnahme, Neue Zeitschrift für Strafrecht 2004, S. 57–64, (zit.: *Demko,* NStZ 2004, Seite)

Dencker, Friedrich: Anm. zu BGH, Urteil vom 10.08.1994 – 3 StR 53/94, Strafverteidiger 1995, S. 232–236, (zit.: *Dencker*, StV 1995, Seite)

Dencker, Friedrich: Verwertungsverbote im Strafprozess, Köln 1977, (zit.: *Dencker*, Verwertungsverbote im Strafprozess, Seite)

Denninger, Erhard: Der „große Lauschangriff" auf dem Prüfstand der Verfassung, Gedächtnisschrift für Hans Lisken, S. 13–24, Berlin 2004, (zit.: GS-Lisken/*Denninger*, Seite)

Denninger, Erhard: Verfassungsrechtliche Grenzen des Lauschens – Der „große Lauschangriff" auf dem Prüfstand der Verfassung, Zeitschrift für Rechtspolitik 2004, S. 101–104, (zit.: *Denninger*, ZRP 2004, Seite)

Derin, Benjamin / Golla, Sebastian: Der Staat als Manipulant und Saboteur der IT-Sicherheit? Die Zulässigkeit von Begleitmaßnahmen zu „Online-Durchsuchung" und Quellen-TKÜ, Neue Juristische Wochenschrift 2019, S. 1111–1116, (zit.: *Derin/Golla*, NJW 2019, Seite)

Desoi, Monika / Knierim, Antoine: Intimsphäre und Kernbereichsschutz, Die öffentliche Verwaltung 2011, S. 398–405, (zit.: *Desoi/Knierim*, DÖV 2011, Seite)

Dölling, Dieter / Duttge, Gunnar / König, Stefan / Rössner, Dieter (Hrsg.): Handkommentar Gesamtes Strafrecht, 4. Auflage, Baden-Baden 2017, (zit.: *Bearbeiter* in: HK-GS, §, Rn.)

Dornach, Markus: Ist der Strafverteidiger aufgrund seiner Stellung als "Organ der Rechtspflege" Mitgarant eines justizförmigen Strafverfahrens?, Neue Zeitschrift für Strafrecht 1995, S. 57–63, (zit.: *Dornach*, NStZ 1995, Seite)

Dreier, Horst (Hrsg.): Grundgesetz Kommentar, 3. Auflage, Band I, Tübingen 2013, (zit.: *Bearbeiter* in: Dreier-GG, Art., Rn.)

DSRI-Tagungsband 2019, S. 497–511, (zit.: *Ametsbichler*, DSRITB 2019, Seite)

Dürr, Maximilian: Der Schutz des allgemeinen Persönlichkeitsrechts nach dem Urteil zum Bundeskriminalamtsgesetz – wie viel Sicherheit ist zum Wohle der Freiheit notwendig?, Juristische Arbeitsblätter 2019, S. 432–440, (zit.: *Dürr*, JA 2019, Seite)

Eberhard, Schmidt: Die Verletzung der Belehrungspflicht gem. § 55 II StPO als Revisionsgrund, Juristenzeitung 1958, S. 596–601, (zit.: *Schmidt*, JZ 1958, Seite)

Eberling, Werner: Beitrag „Serverless mit Alexa – Skills mit AWS Lambda entwickeln", informatik-aktuell.de vom 29.01.2019, (zuletzt abgerufen am 31.10.2021) (zit.: *Eberling*, Serverless mit Alexa, https://www.informatik-aktuell.de/betrieb/server/serverless-mit-alexa-skills-mit-aws-lambda-entwickeln.html#top)

Eckhardt, Jens: Anm. zu BGH: Positionsmeldung durch Mobiltelefon, Beschluss vom 21. Februar 2001 – 2 BGs 42/2001, Computer und Recht 2001, S. 385–388, (zit.: *Eckhardt*, CR 2001, Seite)

Eckhardt, Sebastian: Private Ermittlungsbeiträge im Rahmen der staatlichen Strafverfolgung, Frankfurt 2009, (zit.: *Eckhardt,* Private Ermittlungsbeiträge, Seite)

Eder, Florian: Beweisverbote und Beweislast im Strafprozess, München 2015, (zit.: *Eder*, Beweisverbote, Seite)

Eidam, Lutz: Überwachung der Internetnutzung im Ermittlungsverfahren, zgl. Anmerkung zu BVerfG Beschluss vom 6.7.2016 – 2 BvR 1454/13, Neu Juristische Wochenschrift 2016, S. 3511–3512, (zit.: *Eidam*, NJW 2016, Seite)

Eifert, Martin: Informationelle Selbstbestimmung im Internet – Das BVerfG und die Online-Durchsuchung, Neue Zeitschrift für Verwaltungsrecht 2008, S. 521–523, (zit.: *Eifert*, NVwZ 2008, Seite)

Eisenberg Ulrich / Nischan, Anett: Strafprozessualer Zugriff auf digitale multimediale Videodienste, Juristische Zeitung 1997, S. 74–83, (zit.: *Eisenberg/Nischan*, JZ 1997, Seite)

Eisenberg, Ulrich: Beweisrecht der StPO, 10. Auflage, München 2017, (zit.: *Eisenberg*, Beweisrecht der StPO, Rn.)

Eisenmenger, Florian: Die Grundrechtsrelevanz »virtueller Streifenfahrten« – dargestellt am Beispiel ausgewählter Kommunikationsdienste des Internets, Berlin 2017 (zit.: *Eisenmenger*, Die Grundrechtsrelevanz virtueller Streifenfahrten, Seite)

Ellbogen, Klaus: Die Fluchttagebücher Frank Schmökel und ihre Verwertbarkeit im Strafprozess, Neue Zeitschrift für Strafrecht 2001, S. 460–465, (zit.: Ellbogen, NStZ 2001, Seite)

Ellbogen, Klaus: Verwertungsverbot bei Selbstgesprächen, Neue Zeitschrift für Strafrecht 2006, S. 180–181, (zit.: Ellbogen, NStZ 2006 Seite)

Epping, Volker: Grundrechte, 9. Auflage, Berlin 2021, (zit.: *Epping*, Grundrechte, Rn.)

Erb, Volker / Esser, Robert / Franke, Ulrich / Graalmann-Scheerer, Ulrich / Hilger, Hans / Ignor, Alexander (Hrsg.): Die Strafprozessordnung und das Gerichtsverfassungsgesetz – Löwe-Rosenberg Großkommentar, 27. Auflage / Band 1, Einleitung; §§ 1–47, Berlin 2016 (zit.: *Bearbeiter* in: LR-StPO, §, Rn.)

Erb, Volker / Esser, Robert / Franke, Ulrich / Graalmann-Scheerer, Ulrich / Hilger, Hans / Ignor, Alexander (Hrsg.): Die Strafprozessordnung und das Gerichtsverfassungsgesetz- Löwe-Rosenberg Großkommentar, 27. Auflage / Band 2, §§ 48–93 StPO, Berlin 2018, (zit.: *Bearbeiter* in: LR-StPO, §, Rn.)

Erb, Volker / Esser, Robert / Franke, Ulrich / Graalmann-Scheerer, Ulrich / Hilger, Hans / Ignor, Alexander (Hrsg.): Die Strafprozessordnung und das Gerichtsverfassungsgesetz- Löwe-Rosenberg Großkommentar, 27. Auflage / Band 3, §§ 94–111a StPO, Berlin 2019, (zit.: *Bearbeiter* in: LR-StPO, §, Rn.)

Erb, Volker / Esser, Robert / Franke, Ulrich / Graalmann-Scheerer, Ulrich / Hilger, Hans / Ignor, Alexander (Hrsg.): Die Strafprozessordnung und das Gerichtsverfassungsgesetz- Löwe-Rosenberg Großkommentar, 27. Auflage / Band 4, §§ 112–136a StPO, Berlin 2019, (zit.: *Bearbeiter* in: LR-StPO, §, Rn.)

Erb, Volker / Esser, Robert / Franke, Ulrich / Graalmann-Scheerer, Ulrich / Hilger, Hans / Ignor, Alexander (Hrsg.): Die Strafprozessordnung und das Gerichtsverfassungsgesetz- Löwe-Rosenberg Großkommentar, 27. Auflage / Band 6, Berlin 2020, §§ 212–255a StPO, (zit.: *Bearbeiter* in: LR-StPO, §, Rn.)

Erb, Volker: Beweisverwertungsverbote zum Nachteil des Beschuldigten, Goltdammers Archiv 2017, S. 113–129, (zit.: *Erb*, GA 2017, Seite)

Ernst, Christian / Sturm, Jan: Nichtöffentlich geführte Selbstgespräche und der Schutz des Kernbereichs privater Lebensgestaltung, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2012, S. 374–381, (zit.: *Ernst/Sturm*, HRRS 2012, Seite)

Ernst, Markus: Verarbeitung und Zweckbindung von Informationen im Strafprozess, Berlin 1993, (zit.: *Ernst*, Verarbeitung und Zweckbindung von Informationen, Seite)

Eßer, Martin / Kramer, Philipp / von Lewinski, Kai (Hrsg.): Auernhammer Kommentar DSGVO / BDSG, 7. Auflage, Köln 2020, (zit.: *Bearbeiter* in: Auernhammer-DSGVO/BDSG, § 15, Rn.)

Fährmann, Jan: Digitale Beweismittel und Datenmengen im Strafprozess, Multimedia und Recht 2020, S. 228–233, (zit.: *Fährmann*, MMR 2020, Seite)

Federrath, Hannes: Technik der Cloud, Zeitschrift für Urheber- und Medienrecht 2014, S. 1–3, (zit.: *Federrath*, ZUM 2014, Seite)

Feldmann: Das Tonband als Beweismittel im Strafprozess, Neue Juristische Wochenschrift 1958, S. 1166–1169, (zit.: *Feldmann*, NJW 1958, Seite)

Fezer, Gerhard: Anm. zu Beschluß des BGH v. 27.2.1992 – 5 StR 190/91, Juristische Rundschau 1992, S. 385–387, (zit.: *Fezer*, JR 1992, Seite)

Fezer, Gerhard: Anm. zu BGH Urteil v. 17.11.1989 – 2 StR 418, Juristische Rundschau 1991, S. 85–88, (zit.: *Fezer*, JR 1991, Seite)

Fezer, Gerhard: Anm. zu Schwenn/ Strate, StV 1989, 289, Verstoß gegen Grundsatz der Öffentlichkeit durch Fernsehaufnahmen, rechtliche Mängel einer Durchsuchung, Strafverteidiger 1989, S. 290–295, (zit.: *Fezer*, StV 1989, Seite)

Fezer, Gerhard: Beschränktes Verwertungsverbot bei Verstoß gegen Benachrichtigungspflicht, zugleich Anm. zu BGH, Beschluss vom 17. 2. 2009 – 1 StR 691/08, Neue Zeitschrift für Strafrecht 2009, S. 524–525, (zit.: *Fezer*, NStZ 2009, Seite)

Fezer, Gerhard: Fortwirkungen des Einsatzes verbotener Vernehmungsmethoden, Anforderungen an Revisionsbegründung, zugleich Anm. zu BGH, Beschluss vom 20.12.1995 – 5 StR 445/95, Strafverteidiger 1997, S. 57–59, (zit.: *Fezer*, StV 1997, Seite)

Fezer, Gerhard: Überwachung der Telekommunikation und Verwertung eines Raumgesprächs, Neue Zeitschrift für Strafrecht 2003, S. 625–630, (zit.: *Fezer*, NStZ 2003, Seite)

Fezer, Gerhard: Zur Verwertung der Aussage eines Mitgefangenen, der einen Beschuldigten auf polizeiliche Veranlassung "aushorchen" sollte, zugleich Anm. zu BGH, Urteil vom 28.04.1987 – 5 StR 666/86, Juristenzeitung 1987, S. 937–939, (zit.: *Fezer*, JZ 1987, Seite)

Finger, Thorsten: Prozessuale Beweisverbote – Eine Darstellung ausgewählter Fallgruppen, Juristische Arbeitsblätter 2006, S. 529–539, (zit.: *Finger*, JA 2006, Seite)

Fink, Gudrun: Intimsphäre und Zeugenpflicht, Baden-Baden 2015, (zit.: *Fink*, Intimsphäre und Zeugenpflicht, Seite)

Fischer, Thomas: Strafgesetzbuch, 68. Auflage, München 2021, (zit.: *Fischer*-StGB, §, Rn.)

Fischinger, Philipp: Der Grundrechtsverzicht, Juristische Schulung 2008, S. 808–813, (zit.: *Fischinger*, JuS 2008, Seite)

Fleischmann, Klaus: Verwertbarkeit eines aufgezeichneten Selbstgespräches eines Beschuldigten im Strafverfahren, zugleich Anm. zu BGH Urteil vom 22.12.2011 – 2 StR 509/10, Neue Justiz 2012, S. 218–219, (zit.: *Fleischmann*, NJ 2012, Seite)

Flöhr, Andreas: Zur Berücksichtigung hypothetischer Kausalitätsverläufe im Strafprozessrecht, Juristische Ausbildung 1995, S. 131–134, (zit.: *Flöhr*, Jura 1995, Seite)

Fox, Dirk: Realisierung, Grenzen und Risiken der Online-Durchsuchung, Datenschutz und Datensicherheit 2007, S. 827–834, (zit.: *Fox*, DuD 2007, Seite)

Fox, Dirk: Stellungnahme zur „Online-Durchsuchung" Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, Karlsruhe 2007, abrufbar unter: https://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf, (zuletzt abgerufen am 31.10.2021) (zit.: *Fox*, Stellungnahme, Seite)

Freiling, Felix / Safferling, Christoph / Rückert, Christian:Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, Juristische Rundschau 2018, S. 9–22, (zit.: *Freiling/Safferling/Rückert*, JR 2018, Seite)

Freiling, Felix: Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, Mannheim 2007, abrufbar unter: https://faui1-files.cs.fau.de/filepool/publications/stellungnahme-online-durchsuchung.pdf, (zuletzt abgerufen am 31.10.2021) (zit.: *Freiling*, Stellungnahme, Seite)

Freund, Georg: Verurteilung und Freispruch bei Verletzung der Schweigepflicht eines Zeuge, Goltdammers Archiv 1993, S. 49–66, (zit.: *Freund*, GA 1993, Seite)

Gaede, Karsten: Beweisverbote zur Wahrung des fairen Strafverfahrens in der Rechtsprechung des EGMR insbesondere bei verdeckten Ermittlungen, Juristische Rundschau 2009, S. 493–502, (zit.: *Gaede*, JR 2009, Seite)

Gaede, Karsten: Das Verbot der Umgehung der EMRK durch den Einsatz von Privatpersonen bei der Strafverfolgung, Strafverteidiger 2004, S. 46–53, (zit.: *Gaede*, StV 2004, Seite)

Gaede, Karsten: Der grundrechtliche Schutz gespeicherter E-Mail beim Provider und ihre weltweite strafprozessuale Überwachung, Strafverteidiger 2009, S. 96–102, (zit.: *Gaede*, StV 2009, Seite)

Gähler, Sven: Strafprozessuale Ermittlungsmaßnahmen bei Datenübertragung im Cloud-Computing, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2016, S. 340–349, (zit.: *Gähler*, HRRS 2016, Seite)

Geipel, Andreas: Handbuch der Beweiswürdigung, 3. Auflage, Bonn 2017, (zit.: *Geipel*, Handbuch der Beweiswürdigung, § 25, Rn.)

Gercke, Björn / Julius, Karl-Peter / Temming, Dieter / Zöller, Mark (Hrsg.): Heidelberger Kommentar Strafprozessordnung, 6. Auflage, Heidelberg 2019, (zit.: *Bearbeiter* in: HK-StPO, §, Rn.)

Gercke, Björn: Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, Berlin 2001, (zit.: *Gercke*, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, Seite)

Gercke, Björn: Der Kernbereich privater Lebensgestaltung als absolute Grenze der Wahrheitsermittlung im Strafverfahren, Goltdammers Archiv 2015, S. 339–350, (zit.: *Gercke*, GA 2015, Seite)

Gercke, Björn: Strafverfolgung im Internet: Das Strafprozessrecht und seine Grenzen, Goltdammers Archiv 2012, S. 480–490, (zit.: *Gercke*, GA 2012, Seite)

Gercke, Marco /Brunst, Philipp: Praxishandbuch Internetstrafrecht, 1. Auflage, Stuttgart 2009, (zit.: *Bearbeiter* in: Gercke/Brunst, Internetstrafecht, Rn.)

Gercke, Marco: Anm. zu Urt. des BGH vom 14. 3. 2003 – 2 StR 341/02, Juristische Rundschau 2004, S. 347–349, (zit.: *Gercke*, JR 2004, Seite)

Gercke, Marco: Der Einsatz softwarebasierter Ermittlungsinstrumente zum heimlichen Zugriff auf Computerdaten, Computer und Recht 2007, S. 245–253, (zit.: *Gercke*, CR 2007, Seite)

Gercke, Marco: Der unterbliebene Schritt vom Computer- zum Internetstrafrecht, Anwaltsblatt 2012, S. 709–713, (zit.: *Gercke*, AnwBl 2012, Seite)

Gercke, Marco: Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden, Multimedia und Recht 2008, S. 291–298, (zit.: *Gercke*, MMR 2008, Seite)

Gerhards, Julia: (Grund-)Recht auf Verschlüsselung, Baden-Baden 2010, (zit.: *Gerhards*, Recht auf Verschlüsselung, Seite)

Giebichenstein, Rüdiger: Chancen und Risiken beim Einsatz von Cloud Computing in der Rechnungslegung, Betriebs-Berater 2011, S. 2218–2224, (zit.: *Giebichenstein*, BB 2011, Seite)

Giedke, Anne: Cloud Computing: Eine wirtschaftsrechtliche Analyse mit besonderer Berücksichtigung des Urheberrechts, München 2013, (zit.: *Giedke*, Cloud Computing, Seite)

Gless, Sabine / Wennekers, Jan: Anm. BGH, Urt. v. 18. 12. 2008 – 4 StR 455/08, Juristische Rundschau 2009, 383–385, (zit.: *Gless/Wennekers*, JR 2009, Seite)

Gless, Sabine: Beschränktes Verwertungsverbot bei Verstoß gegen Benachrichtigungspflicht, zugleich Anm. zu BGH, Beschluss vom 17. 2. 2009 – 1 StR 691/08, Neue Zeitschrift für Strafrecht 2010, S. 98–100, (zit.: *Gless*, NStZ 2010, Seite)

Gless, Sabine: Wenn das Haus mithört: Beweisverbote im digitalen Zeitalter, Strafverteidiger 2018, S. 671–678, (zit.: *Gless*, StV 2018, Seite)

Godenzi, Gunhild: Das strafprozessuale Verbot staatlicher Beweismittelhehlerei, Goltdammers Archiv 2008, S. 500–515, (zit.: *Godenzi*, GA 2008, Seite)

Göldner, Detlef: Verfassung, Rechtsfortbildung und Lücke, Festschrift für Karl Larenz zum 80. Geburtstag, S. 199–210, München 1983, (zit.: FS-Larenz/*Bearbeiter*, Seite)

Götting, Susanne: Beweisverwertungsverbote in Fällen nicht geregelter Ermittlungstätigkeit, Frankfurt 2001, (zit.: *Götting*, Beweisverwertungsverbote in Fällen nicht geregelter Ermittlungstätigkeit, Seite)

Grasnick, Walter: Polizeiliche Beschuldigtenvernehmung ohne „qualifizierte" Belehrung, Neue Zeitschrift für Strafrecht 2010, S. 158–159, (zit.: *Grasnick*, NStZ 2010, Seite)

Graßie, Christian / Hiéramente, Mayeul: Praxisprobleme bei der IT-Durchsuchung, Compliance Berater 2019, S. 191–196, (zit.: *Graßie/Hiéramente*, CB 2019, Seite)

Grenzer, Matthis /Heitmüller, Niklas: Zur Problematik des Personenbezuges beim Cloud Computing, Privacy in Germany 2014, S. 221–230, (zit.: *Grenzer/Heitmüller*, PinG 2014, Seite)

Greve, Holger: Acces-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, Berlin 2012, (zit.: *Greve*, Acces-Blocking, Seite)

Gropp, Walter: Zur Verwertbarkeit eigenmächtig aufgezeichneter (Telefon-) Gespräche, Strafverteidiger 1989, S. 216–228, (zit.: *Gropp*, StV 1989, Seite)

Großmann, Sven: Telekommunikationsüberwachung und Online-Durchsuchung: Voraussetzungen und Beweisverbote, Juristische Arbeitsblätter 2019, S. 241–248, (zit.: *Großmann*, JA 2019, Seite)

Großmann, Sven: Zur repressiven Online-Durchsuchung, Goltdammers Archiv 2018, S. 439–456, (zit.: *Großmann*, GA 2018, Seite)

Grözinger, Andreas: Die Überwachung von Cloud-Storage, Köln 2018, (zit.: *Grözinger*, Die Überwachung von Cloud-Storage, Seite)

Grözinger, Andreas: Heimliche Zugriffe auf den Datenbestand einer Mailbox, Goltdammers Archiv 2019, S. 441–454, (zit.: *Grözinger*, GA 2019, Seite)

Grözinger, Andreas: Heimliche Zugriffe auf die Cloud – Befugnis zur Plünderung eines unermesslichen Datenschatzes?, Strafverteidiger 2019, S. 406–412, (zit.: *Grözinger*, StV 2019, Seite)

Grözinger, Andreas: Praxiskommentar zum Beschluss des BGH vom 14.10.2020 (5 StR 229/19), Neue Zeitschrift für Strafrecht 2021, S. 358–360, (zit.: Grözinger, NStZ 2021, Seite)

Grüner, Gerhard: Revisibilität und Beweisverwertungsverbote im Strafprozess, Leipzig 1997, (Grüner, Revisibilität und Beweisverwertungsverbote, Seite)

Grunewald, Barbara / Maier-Reimer Georg / Westermann, Harm Peter (Hrsg.): Erman-Kommentar BGB, 16. Auflage, Köln 2020, (zit.: *Bearbeiter* in: Erman-BGB, §, Rn.)

Grünwald, Andreas / Döpkens, Harm-Randolf: Cloud Control? Regulierung von Cloud Computing-Angeboten, Multimedia und Recht 2011, S. 287–290, (zit.: *Grünwald/Döpkens*, MMR 2011, Seite)

Grünwald, Gerald: Beweisverbote im Strafverfahren, Juristenzeitung 1966, S. 489–501, (zit.: *Grünwald*, JZ 1966, Seite)

Grünwald, Gerald: Das Beweisrecht der Strafprozessordnung, Baden-Baden 1993, (zit.: *Grünwald*, Das Beweisrecht, Seite)

Grünwald, Gerald: Unzulässige Vernehmungsmethoden, Fernwirkung von Beweisverwertungsverboten, zugleich Anm. zu BGH, Urteil vom 28.04.1987 – 5 StR 666/86, Strafverteidiger 1987, S. 470–473, (zit.: *Grünwald*, StV 1987, Seite)

Grützner, Thomas / Jakob, Alexander: Compliance von A bis Z, 2. Auflage, München 2015, (zit.: *Grützner/Jakob*, Compliance von A-Z, Begriff)

Güntge, Georg-Friedrich: Beweisverwertungsverbote zu Ungunsten eines (Mit-)Angeklagten?, Strafverteidiger 2005, S. 403–406, (zit.: *Güntge*, StV 2005, Seite)

Gusy, Christoph: Lauschangriff und Grundgesetz, Juristische Schulung 2004, S. 457–462, (zit.: *Gusy*, JuS 2004, Seite)

Gusy, Christoph: Verfassungsfragen des Strafprozeßrechts, Strafverteidiger 2002, S. 153–160, (zit.: *Gusy*, StV 2002, Seite)

Guttenberg, Ulrich: Die heimliche Überwachung von Wohnungen, Neue Juristische Wochenschrift 1993, S. 567–576, (zit.: *Guttenberg*, NJW 1993, Seite)

Haas, Andreas / Hofmann, Anette: Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit, 2. Fassung, Hohenheim 2013, (zit.: *Haas/Hofmann*, Risiken aus der Cloud, Seite)

Haas, Günter: Der „Große Lauschangriff" – klein geschrieben, Neue Juristische Wochenschrift 2004, S. 3082–3084, (zit.: *Haas*, NJW 2004, Seite)

Habetha, Jörg: Anm. zu BGH, Urt. v. 22.12.2011 – 2 StR 509/10 (Verwertungsverbot bzgl. eines abgehörten Selbstgesprächs), Zeitschrift für Wirtschaftsstrafrecht und Haftung im Unternehmen 2012, S. 165 – 166, (zit.: *Habetha*, ZWH 2012, Seite)

Haffke, Bernhard: Schweigepflicht, Verfahrensrevision und Beweisverbot, Goltdammers Archiv 1973, S. 65–84, (zit.: *Haffke*, GA 1973, Seite)

Hamm, Rainer: Die Revision in Strafsachen, 7. Auflage, Berlin 2010, (zit.: *Hamm*, Die Revision in Strafsachen, Seite)

Hamm, Rainer: Staatliche Hilfe bei der Suche nach Verteidigern – Verteidigerhilfe zur Begründung von Verwertungsverboten, Neue Juristische Wochenschrift 1996, S. 2185–2190, (zit.: *Hamm*, NJW 1996, Seite)

Hanack, Ernst-Walter: Die Rechtsprechung des Bundesgerichtshofs zum Strafverfahrensrecht, Juristenzeitung 1971, S. 126–128, (zit.: *Hanack*, JZ 1971, Seite)

Hannich, Rolf (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung, 9. Auflage, München 2019, (zit.: *Bearbeiter* in: KK-StPO, §, Rn.)

Hansen, Markus / Pfitzmann, Andreas: Technische Grundlagen von Online-Durchsuchung und Beschlagnahme, Deutsche Richterzeitung 2007, S. 225–228, (zit.: *Hansen/Pfitzmann*, DRiZ 2007, Seite)

Hansen, Sven: Meine Musik mobil, Magazin für Computertechnik, 2011, Heft 23 S. 98–105, (zit.: *Hansen*, c/t 2011, Heft 23, Seite)

Harnisch, Stefan / Pohlmann, Martin: Strafprozessuale Maßnahmen bei Mobilfunkendgeräten, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2009, S. 202–217, (zit.: Harnisch/Pohlmann, HRRS 2009, Seite)

Harris, Kenneth: Verwertungsverbot für mittelbar erlangte Beweismittel, Strafverteidiger 1991, S. 313–322, (zit.: *Harris*, StV 1991, Seite)

Hassemer, Winfried / Matussek, Karin: Das Opfer als Verfolger – Ermittlungen des Verletzten im Strafverfahren, Frankfurt 1996, (zit.: *Hassemer/Matussek*, Das Opfer als Verfolger, Seite)

Hauck, Pierre: Heimliche Strafverfolgung und Schutz der Privatheit, Tübingen 2014, (*Hauck*, Heimliche Strafverfolgung, Seite)

Hauck, Pierre: Kritische Anmerkungen zur Regelung der Bestandsdatenauskunft in § 100j StPO, Strafverteidiger 2014, S. 360–366, (zit.: *Hauck*, StV 2014, Seite)

Haverkamp, Rita: Die akustische Wohnraumüberwachung – ein unzulässiger Eingriff in den unantastbaren Kernbereich privater Lebensgestaltung?, Juristische Ausbildung 2010, S. 492–498, (zit.: *Haverkamp*, Jura 2010, Seite)

Heger, Martin / Pohlreich, Erich: Strafprozessrecht, 2. Auflage, Stuttgart 2018, (zit.: *Heger/Pohlreich*, Strafprozessrecht, Rn.)

Heghmanns, Michael: Beweisverwertungsverbote, Zeitschrift für Internationale Strafrechtsdogmatik 2016, S. 404–415, (zit.: *Heghmanns*, ZIS 2016, Seite)

Heidrich, Joerg / Maekeler, Nicolas: Alexa, darfst du das? Rechtliche Probleme durch Sprachassistenten, Magazin für Computertechnik 2017, Heft 22, S. 86–87, (zit.: *Heidrich/Maekeler*, c´t 2017, Heft, Seite)

Heinrich, Bernd: Rügepflichten in der Hauptverhandlung und Disponibilität strafverfahrensrechtlicher Vorschriften, Zeitschrift für die gesamte Strafrechtswissenschaft 2000, S. 398 – 428, (zit.: *Heinrich*, ZStW 2000, Seite)

Heinson, Dennis: IT-Forensik. Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen, Tübingen 2015, (zit.: Heinson, IT-Forensik, Seite)

Heller, Piotr:Beitrag „Alexa, war es Mord?", FAZ.net, vom 08.05.2017, abrufbar unter: http://www.faz.net/aktuell/physik-mehr/internet-der-dinge-wenn-smarte-geraete-zu-zeugen-werden-15003037.html (zuletzt abgerufen am 30.10.2021), (zit.: *Heller*, Alexa, war es Mord?, http://www.faz.net/aktuell/physik-mehr/internet-der-dinge-wenn-smarte-geraete-zu-zeugen-werden-15003037.html)

Hennrich, Thorsten: Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz, Berlin 2016, (zit.: *Hennrich*, Cloud Computing, Seite)

Hennrich, Thorsten: Compliance in Clouds, Computer und Recht 2011, S. 546–552, (zit.: *Hennrich*, CR 2011, Seite)

Henrichs, Axel / Wilhelm, Jörg: Polizeiliche Ermittlungen in sozialen Netzwerken, Kriminalistik 2010, S. 30–37, (zit.: *Henrichs/Wilhelm*, Kriminalistik 2010, Seite)

Herrmann, Joachim: Aufgaben und Grenzen des Beweisverwertungsverbote, Festschrift Hans-Heinrich Jescheck zum 70. Geburtstag, S. 1291–1310, Berlin 1985, (zit.: FS-Jescheck/*Herrmann*, Seite)

Herrmann, Klaus / Soiné, Michael:Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, Neue Juristische Wochenschrift 2011, S. 2922–2928, (zit.: *Herrmann/Soiné*, NJW 2011, Seite)

Herzog, Roman / Scholz, Rupert / Herdegen, Matthias / Klein, Hans (Hrsg.): Maunz / Dürig Grundgesetz Kommentar, Stand 94. Ergänzungslieferung, München 2021, (zit*.: Bearbeiter* in: Maunz/Dürig-GG, Art, Rn.)

Heuchemer, Michael / Paul, Thomas: Die Strafbarkeit unbefugter Bildaufnahmen – Tatbestandliche Probleme des § 201a StGB, Juristische Arbeitsblätter 2006, S. 616–620, (zit.: *Heuchemer/Paul*, JA 2006, Seite)

Heydn, Truiken: Software as a Service (SaaS): Probleme und Vertragsgestaltung, Multimedia und Recht 2020, S. 435–440, (zit.: *Heydn*, MMR 2020, Seite)

Hiéramente, Mayeul / Fenina, Patrick: Telekommunikationsüberwachung und Cloud Computing, Strafverteidiger Forum 2015, S. 365–374, (zit.: *Hiéramente/Fenina*, StraFo 2015, Seite)

Hiéramente, Mayeul: Der irrlichternde 5. Strafsenat – Kein heimlicher Zugriff auf Alt-Emails nach § 100a StPO, zugleich eine Anmerkung zu BGH, Beschl. v. 14.10.2020 – 5 StR 229/19, Journal der Wirtschaftsstrafrechtlichen Vereinigung e.V. 2021, S. 19–23, (zit.: *Hiéramente*, WiJ 2021, Seite)

Hiéramente, Mayeul: Durchsuchung und „Durchsicht" der Unternehmens-IT – Betrachtungen zu §§ 103, 110 StPO, Zeitschrift für Wirtschafts- und Steuerstrafrecht 2016, S. 432–440, (zit.: *Hiéramente*, wistra 2016, Seite)

Hiéramente, Mayeul: Legalität der strafprozessualen Überwachung des Surfverhaltens, Strafverteidiger Forum 2013, S. 96–102, (zit.: *Hiéramente*, StraFo 2013, Seite)

Hiéramente, Mayeul:Surfen im Internet doch Telekommunikation im Sinne des § 100a StPO?, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2016, S. 448–452, (zit.: *Hiéramente*, HRRS 2016, Seite)

Hilber, Marc (Hrsg.):Handbuch Cloud Computing, 1. Auflage, Köln 2014, (zit.: *Bearbeiter* in: Hilber, Handbuch Cloud Computing, Teil, Rn.)

Hilgendorf, Eric / Valerius, Brian: Computer- und Internetstrafrecht, 2. Auflage, Berlin 2012, (zit.: *Hilgendorf/Valerius*, Internetstrafrecht, Rn.)

Hilger, Hans: Über den „Richtervorbehalt" im Ermittlungsverfahren, Juristische Rundschau 1990, S. 485–489, (zit.: *Hilger*, JR 1990, Seite)

Hoeren, Thomas / Sieber, Ulrich / Holznagel, Bernd (Hrsg.): Handbuch Multimedia-Recht, Stand: April 2020 – 52. Ergänzungslieferung, München 2019, (zit.: *Bearbeiter* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil, Rn.)

Hoeren, Thomas: Das Telemediengesetz, Neue Juristische Wochenschrift 2007, S. 801–806, (zit.: *Hoeren*, NJW 2007, Seite)

Hoffmann-Riem, Wolfgang: Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, Juristenzeitung 2008, S. 1009–1022, (zit.: *Hoffmann-Riem*, JZ 2008, Seite)

Hofmann, Hans / Henneke, Hans-Günther (Hrsg.): Schmidt-Bleibtreu / Hofmann / Henneke – Kommentar zum Grundgesetz, 14. Auflage, Köln 2018, (zit: *Bearbeiter* in: SHH, Art., Rn.)

Hofmann, Manfred: Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?, Neue Zeitschrift für Strafrecht 2005, S. 121–125, (zit.: *Hofmann*, NStZ 2005, Seite)

Hohmann-Dennhardt, Christine: Freiräume – Zum Schutz der Privatheit, Neue Juristische Wochenschrift 2006, S. 545–549, (zit.: *Hohmann-Dennhardt*, NJW 2006, Seite)

Hombrecher, Lars: Rechtsverstöße im Ermittlungsverfahren als Gegenstand der Revision – Grundlagen und aktuelle Rechtsprechung zu Beweisverwertungsverboten, Juristische Arbeitsblätter 2016, S. 457–463, (zit.: *Hombrecher*, JA 2016, Seite)

Hömig, Dieter / Wolff, Heinrich Amadeus: Grundgesetz Handkommentar, 12. Auflage, Baden-Baden 2018, (zit.: *Bearbeiter* in: Hömig/Wolff-GG, Art., Rn.)

Hörner, Thomas: Marketing mit Sprachassistenten, Wiesbaden 2019, (zit.: *Hörner*, Marketing mit Sprachassistenten, Seite)

Hornick, Andreas: Staatlicher Zugriff auf elektronische Medien, Strafverteidigerforum 2008, S. 281–286, (zit.: *Hornick*, StraFo 2008, Seite)

Hornung, Gerit: Die Krypto-Debatte: Wiederkehr einer Untoten, Multimedia und Recht 2015, S. 145–146, (zit.: *Hornung*, MMR 2015, Seite)

Hornung, Gerit: Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, Multimedia und Recht 2004, S. 3–8, (zit.: *Hornung*, MMR 2004, Seite)

Hornung, Gerrit / Sädtler, Stephan: Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing, Computer und Recht 2012, S. 638–645, (zit.: *Hornung/Sädtler*, CR 2012, Seite)

Huber, Bertold: Trojaner mit Schlapphut – Heimliche „Online-Durchsuchung" nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz, Neue Zeitschrift für Verwaltungsrecht 2007, S. 880–884, (zit.: *Huber*, NVwZ 2007, Seite)

Huber, Peter / Voßkuhle, Andreas (Hrsg.): v. Mangoldt/Klein/Stark – Kommentar zum Grundgesetz, 7. Auflage, München 2018, (zit.: *Bearbeiter* in: v. Mangoldt/Klein/Stark, Art., Rn.)

Hufen, Friedhelm: Die Menschenwürde, Art. 1 GG, Juristische Schulung 2010, S. 1–10, (zit.: *Hufen*, JuS 2010, Seite)

Hufen, Friedhelm: Staatsrecht II – Grundrechte, 8. Auflage, München 2020, (zit.: *Hufen*, Grundrechte, §, Rn.)

Hüls, Silke: Der Richtervorbehalt – seine Bedeutung für das Strafverfahren und die Folgen von Verstößen, Zeitschrift für Internationale Strafrechtsdogmatik 2009, S. 160–169, (zit.: *Hüls*, ZIS 2009, Seite)

Jäger, Christian: Beweiserhebungs- und Beweisverwertungsverbote als prozessuale Regelungsinstrumente im strafverfolgenden Rechtsstaat, Goltdammers Archiv 2008, S. 473–499, (zit.: *Jäger*, GA 2008, Seite)

Jäger, Christian: Beweisverwertung und Beweisverwertungsverbote im Strafprozess, München 2003, (zit.: *Jäger,* Beweisverwertung und Beweisverwertungsverbote, Seite)

Jäger, Christian: Du sollst nicht von Dritten profitieren!, Juristische Arbeitsblätter 2017, S. 74–76, (zit.: *Jäger*, JA 2017, Seite)

Jäger, Christian: Staatsanwaltschaftliche Durchsuchungsanordnung bei verzogener Gefahr, Juristische Ausbildung 2016, S. 710–712, (zit.: *Jäger*, JA 2016, Seite)

Jahn, Matthias / Dallmeyer, Jens: Zum heutigen Stand der beweisrechtlichen Berücksichtigung hypothetischer Ermittlungsverläufe im deutschen Strafverfahrensrecht, Neue Zeitschrift für Strafrecht 2005, S. 297–304, (zit.: *Jahn/Dallmeyer*, NStZ 2005, Seite)

Jahn, Matthias / Geck, Elena: Tagebuchfall revisited – Der Bundesgerichtshof, die Gedankenfreiheitund ein Selbstgespräch im Auto, Juristenzeitung 2012, S. 561–567, (zit.: *Jahn/Geck*, JZ 2012, Seite)

Jahn, Matthias: Strafprozessrecht – Unverwertbarkeit eines im Krankenzimmer abgehörten Selbstgesprächs des Angeklagten, Juristische Schulung 2006, S. 91–92, (zit.: *Jahn*, JuS 2006, Seite)

Jahn, Matthias: Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus, Verhandlungen des 67. Deutschen Juristentages, C1-C128, Erfurt 2008, (zit.: *Jahn*, Gutachten dt. Juristentag, Seite)

Jahn, Matthias: Grundfragen und aktuelle Probleme der Beweisverwertung im Straf- und Steuerstrafverfahren, Festschrift für Heinz Stöckel zum 70. Geburtstag, S. 259–286, Berlin 2010, (zit.: FS-Stöckel/*Jahn*, Seite)

Jahn, Matthias: Strafprozessrecht – Ambivalenz von Beweisverwertungsverboten – „Mühlenteichtheorie", Juristische Schulung 2005, S. 1121–1123, (zit.: *Jahn*, JuS 2005, Seite)

Jahn, Matthias: Strafverfolgung um jeden Preis, Strafverteidiger Forum 2011, S. 117–128, (zit.: *Jahn*, StraFo 2011, Seite)

Jansen, Scarlett: Strafprozessuale Beweisverwertung von privatem Videomaterial, insbesondere von Dash- und Bodycams, Strafverteidiger 2019, S. 578–584, (zit.: *Jansen*, StV 2019, Seite)

Jescheck, Hans-Heinrich: Beweisverbote im Strafprozess, Verhandlungen des 46. Deutschen Juristentages, Band I: Gutachten, Teil 3B, S. 1–53, München 1966, (zit.: *Jescheck*, 46. DJT, Bd. I, Seite)

Joecks, Wolfgang / Miebach, Klaus (Hrsg.):Münchener Kommentar zum StGB, 4. Auflage, Band 4, München 2021, (zit.: *Bearbeiter* in: MüKo-StGB, §, Rn.)

Joecks, Wolfgang: Strafgesetzbuch Studienkommentar, 11. Auflage, München 2014, (zit.: *Joecks*-Studienkommentar, §, Rn.)

Joerden, Jan: Verbote Vernehmungsmethoden – Grundfragen des § 136a StPO, Juristische Schulung 1993, S. 927–931, (zit.: *Joerden*, JuS 1993, Seite)

Jugl, Benedikt: Fair trial als Grundlage der Beweiserhebung und Beweisverwertung im Strafverfahren, Baden-Baden 2017, (zit.: *Jugl*, Fair trial als Grundlage im Strafverfahren, Seite)

Jurran, Nico / Porteck, Stefan: Gekommen, um zu bleiben – Was wir von Alexa & Co in Zukunft erwarten dürfen, Magazin für Computertechnik 2019, Heft 20, S. 72–73, (zit.: *Jurran/Porteck*, c´t 2019, Heft, Seite)

Jurran, Nico: Fremde Ohren – Amazon, Google und Apple zu mehr Datenschutz bei ihren Sprachassistenten gezwungen, Magazin für Computertechnik 2019, Heft 18, S. 36, (zit.: *Jurran*, c´t 2019, Heft, Seite)

Jurran, Nico: Großer Lauschangriff? Was Alexa & Co. Aufzeichnen und wie diese Daten verarbeitet werden, Magazin für Computertechnik 2018, Heft 23, S. 68, (zit.: *Jurran*, c´t 2018, Heft, Seite)

Kamlah, Ruprecht: Datenüberwachung und Bundesverfassungsgericht, Die öffentliche Verwaltung 1970, S. 361–364, (zit.: *Kamlah*, DÖV 1970, Seite)

Karg, Moritz: Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung, Datenschutz und Datensicherheit 2015, S. 85–88, (zit.: *Karg*, DuD 2015, Seite)

Kasiske, Peter: Fern-, Fort- und Frühwirkung von Beweisverwertungsverboten im Strafprozess, Juristische Ausbildung 2017, S. 16–25, (zit.: *Kasiske*, Jura 2017, Seite)

Kaspar, Johannes: Strafprozessuale Verwertbarkeit nach rechtswidriger privater Beweisbeschaffung, Goltdammers Archiv 2013, S. 206–225, (zit.: *Kaspar,* GA 2013, Seite)

Käß, Robert: Die Einführung der präventiven Telekommunikationsüberwachung im Bayerischen Polizeiaufgabengesetz, Bayerische Verwaltungsblätter 2008, S. 225–234, (zit.: *Käß*, BayVBl 2008, Seite)

Kassing, Daniel: Die Verwertbarkeit von Beweisen bei Verstoß gegen § 105 I 1 StPO, Juristische Schulung 2004, S. 675–678, (zit.: *Kassing*, JuS 2004, Seite)

Kelnhofer, Evelyn: Hypothetische Ermittlungsverläufe im System der Beweisverbote, Berlin 1994, (zit.: *Kelnhofer*, Hypothetische Ermittlungsverläufe, Seite)

Kemper, Martin: Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten, Zeitschrift für Rechtspolitik 2007, S. 105–109, (zit.: *Kemper*, ZRP 2007, Seite)

Kemper, Martin: Die Beschlagnahmefähigkeit von Daten und E-Mails, Neue Zeitschrift für Strafrecht 2005, S. 538–544, (zit.: *Kemper*, NStZ 2005, Seite)

Kian, Bardia:Cloud Computing, Baden-Baden 2016, (zit.: *Kian*, Cloud Computing, Seite)

Kindhäuser, Urs / Neumann, Ulfrid / Paeffgen, Hans Ulrich (Hrsg.): Strafgesetzbuch, 5. Auflage, Baden-Baden 2017, (zit.: *Bearbeiter* in: NK-StGB, §, Rn.)

Kindhäuser, Urs / Schumann, Kay: Strafprozessrecht, 5. Auflage, Baden-Baden 2019, (zit.: *Kindhäuser*, StPO, §, Rn.)

Kingreen, Thorsten / Poscher, Ralf: Grundrechte – Staatsrecht II, 35. Auflage, Heidelberg 2019, (zit.: *Kingreen/Poscher*, Grundrechte, Rn.)

Kleb-Braun, Gabriele: Tagebuchaufzeichnungen als Beweismittel, Computer und Recht 1990, S. 344–352, (zit.: *Kleb-Braun*, CR 1990, Seite)

Kleih, Björn Christian: Die strafprozessuale Überwachung der Telekommunikation, Baden-Baden 2010, (zit.: *Kleih*, Die strafprozessuale Überwachung der Telekommunikation, Seite)

Kleine-Vossbeck, Bernd: Electronic Mail und Verfassungsrecht, Marburg 2000, (zit.: *Kleine-Vossbeck*, Electronic Mail, Seite)

Kleinknecht, Theodor: Die Beweisverbote im Strafprozess, Neue Juristische Wochenschrift 1966, S. 1537–1545, (zit.: *Kleinknecht*, NJW 1966, Seite)

Klemke, Olaf / Elbs, Hansjörgs: Einführung in die Praxis der Strafverteidigung, 4. Auflage, Heidelberg 2019, (zit.: *Klemke/Elbs*, Einführung in die Praxis der Strafverteidigung, Rn.)

Klesczewski, Diethelm: Heimliche Überwachung von Ehegattenbesuchen in der U-Haft, Anmerkung zu BGH, Urteil vom 29.04.2009 – 1 StR 701/08, Strafverteidiger 2010, S. 458–465, (zit.: *Klesczewski*, StV 2010, Seite)

Klesczewski, Diethelm: Strafaufklärung im Internet, Zeitschrift für Strafrechtswissenschaft 2011, S. 737–766, (zit.: *Klesczewski*, ZStW 2011, Seite)

Klug, Ulrich: Referat, Verhandlungen des 46. Deutschen Juristentages, Band II: Referat, Teil F, F 31 – F 61, München 1966, (zit.: *Klug*, 46. DJT, Bd. 2, Seite)

Knauer, Christoph / Kudlich, Hans / Schneider, Hartmut (Hrsg.): Münchener Kommentar zur StPO, 1. Auflage, Band 1 München 2014, Band 2 München 2016, Band 3 München 2018, (zit.: *Bearbeiter* in: MüKo-StPO, §, Rn.)

Knierim, Thomas: Fallrepetitorium zur Wohnraumüberwachung und anderen verdeckten Eingriffen nach neuem Recht, Strafverteidiger 2009, S. 206–212, (zit.: *Knierim*, StV 2009, Seite)

Koch, Arnd: Lauschangriff« via Handy?, Kommunikation & Recht 2004, S. 137–138, (zit.: *Koch*, K&R 2004, Seite)

Kohlhaas, Max: Beweisverbote im Strafprozess, Deutsche Richterzeitung 1966, S. 286–291, (zit.: *Kohlhaas*, DRiZ 1966, Seite)

Kohlhaas, Max: Die Tonbandaufnahme als Beweismittel im Strafprozess, Neue Juristische Wochenschrift 1957, S. 81–85, (zit.: *Kohlhaas*, NJW 1957, Seite)

Kolz, Alexander: Das Selbstgespräch im Krankenzimmer und der „Große Lauschangriff", Neue Juristische Wochenschrift 2005, S. 3248–3250, (zit.: *Kolz*, NJW 2005, Seite)

König, Stefan / Harrendorf, Stefan: Im Spannungsfeld zwischen Rechtsstaat und Kriminalitätsbekämpfung, Anwaltsblatt 2008, S. 566–569, (zit.: *König/Harrendorf*, AnwBl. 2008, Seite)

Koranyi, Johannes: Der Schutz der Wohnung im Strafrecht, Juristische Arbeitsblätter 2014, S. 241–247, (zit.: *Koranyi*, JA 2014, Seite)

Koriath, Heinz: Über Beweisverbote im Strafprozess, Frankfurt 1994, (zit.: *Koriath*, Beweisverbote im Strafprozess, Seite)

Kötter, Matthias: Novellierung der präventiven Wohnraumüberwachung, Die öffentliche Verwaltung 2005, S. 225–234, (zit.: *Kötter*, DÖV 2005, Seite)

Kramer, Bernhard: Heimliche Tonbandaufnahmen im Strafprozeß, Neue Juristische Wochenschrift 1990, S. 1760–1764, (zit.: *Kramer*, NJW 1990, Seite)

Kramer, Bernhard: Unerlaubte Vernehmungsmethoden in der Untersuchungshaft, Juristische Ausbildung 1988, S. 520–525, (zit.: *Kramer*, Jura 1988, Seite)

Kraus, Matthias: Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drs. 18/112727, Karlsruhe 2017, abrufbar unter: https://www.bundestag.de/resource/blob/509046/5aa0ea61c4f3df0429208b5fda260a0a/krauss-data.pdf, (zuletzt abgerufen am 31.10.2021) (zit.: *Kraus*, Stellungnahme, Seite)

Krause, Benjamin: Sicherung von ausländischen E-Mail-Postfächern durch heimliches Einloggen – innovativ oder unzulässig, Kriminalistik 2014, S. 213–217, (zit.: *Krause*, Kriminalistik 2014, Seite)

Krehl, Christoph: Gefahr im Verzug, Juristische Rundschau 2001, S. 491–495, (zit.: *Krehl*, JR 2001, Seite)

Krehl, Christoph: Richtervorbehalt und Durchsuchungen außerhalb gewöhnlicher Dienstzeiten, Neue Zeitschrift für Strafrecht 2003, S. 461–464, (zit.: *Krehl*, NStZ 2003, Seite)

Krekeler, Wilhelm: Beweisverwertungsverbote bei fehlerhaften Durchsuchungen, Neue Zeitschrift für Strafrecht, 1993, S. 263–268, (zit.: *Krekeler*, NStZ 1993, Seite)

Kremer, Sascha / Völkel, Christian:Cloud Storage und Cloud Collaboration als Telekommunikationsdienste, Computer und Recht 2015, S. 501–505, (zit.: *Kremer/Völkel*, CR 2015, Seite)

Krempl, Stefan: Lauschangriff 4.0, Magazin für Computertechnik 2019, Heft 14, S. 36–37, (zit.: *Krempl*, c´t 2019, Heft, Seite)

Kretschmer, Joachim: § 160a StPO – gelungene oder misslungene Gesetzgebung?, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2010, S. 551–558, (zit.: *Kretschmer*, HRRS 2010, Seite)

Krischker, Sven: Das Internetstrafrecht vor neuen Herausforderungen, Würzburg 2014, (zit.: *Krischker*, Das Internetstrafrecht vor neuen Herausforderungen, Seite)

Kroschwald, Stefan: Informationelle Selbstbestimmung in der Cloud, Wiesbaden 2016, (zit.: *Kroschwald*, Informationelle Selbstbestimmung in der Cloud, Seite)

Krüger, Christine: Die sogenannte „stille SMS" im strafprozessualen Ermittlungsverfahren, Zeitschrift für das Juristische Studium 2012, S. 606–613, (zit.: *Krüger*, ZJS 2012, Seite)

Krüger, Hartmut: Anm. zu BVerfG, Beschluss vom 16.6.2009 – 2 BvR 902/06, Multimedia und Recht 2009, S. 680–683, (zit.: *Krüger*, MMR 2009, Seite)

Kruse, Björn / Grzesiek, Mathias: Die Online-Durchsuchung als „digitale Allzweckwaffe" – Zur Kritik an überbordenden Ermittlungsmethoden, Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 2017, S. 331–350, (zit.: *Kruse/Grzesiek*, KritV 2017, Seite)

Kudlich, Hans: Der heimliche Zugriff auf Daten in einer Mailbox: ein Fall der Überwachung des Fernmeldeverkehrs, Juristische Schulung 1998, S. 209–214, (zit.: *Kudlich*, JuS 1998, Seite)

Kudlich, Hans: Die Lehre von der objektiven Zurechnung als Vorbild für die Argumentationslastverteilung bei der Entstehung unselbständiger Beweisverwertungsverbote, Festschrift für Jürgen Wolter zum 70. Geburtstag, S. 995–1008, Berlin 2013, (zit.: FS-Wolter/*Kudlich*, Seite)

Kudlich, Hans: Leider nicht Bescheid gesagt – Unterlassen der Verteidigerbenachrichtigung von einer Beschuldigtenvernehmung, zugleich Anm. zu BGH, Beschluss vom 17. 2. 2009 – 1 StR 691/08, Juristische Arbeitsblätter 2009, S. 660–662, (zit.: *Kudlich*, JA 2009, Seite)

Kudlich, Hans: Mitteilung der Bewegungsdaten eines Mobiltelefons als Überwachung der Telekommunikation, Juristische Schulung 2001, S. 1165–1169, (zit.: *Kudlich*, JuS 2001, Seite)

Kudlich, Hans: Strafverfolgung im Internet, Goltdammers´s Archiv für Strafrecht 2011, S. 193–208, (zit.: *Kudlich*, GA 2011, Seite)

Kudlich, Hans: Telefonate von Krankheit, Sex und Tod – zum Kernbereich privater Lebensgestaltung bei der TKÜ, Festschrift für Thomas Fischer, S. 723–736, München 2018, (zit.: FS-Fischer/*Kudlich*, Seite)

Kühl, Eike: Beitrag „Bei Echo Mord?", zeit.de vom 29.12.2016, abrufbar unter: https://www.zeit.de/digital/datenschutz/2016-12/amazon-echo-mord-aufnahmen-polizei/komplettansicht (zuletzt abgerufen am 31.10.2021), (zit.: *Kühl*, Bei Echo Mord?, https://www.zeit.de/digital/datenschutz/2016-12/amazon-echo-mord-aufnahmen-polizei/komplettansicht

Kühne, Hans-Heiner: Strafprozessrecht, 9. Auflage, Heidelberg 2015, (zit.: *Kühne*, Strafprozessrecht, Rn.)

Kunig, Philip (Hrsg.): Grundgesetz Kommentar, 7. Auflage, München 2021, (zit.: *Bearbeiter* in: v. Münch/Kunig, Art. Rn.)

Küpper, Georg: Tagebücher, Tonbänder und Telefonate, Juristenzeitung 1990, S. 416–424, (zit.: *Küpper*, JZ 1990, Seite)

Kutscha, Martin /Roggan, Fredrik: Große Lauschangriffe im Polizeirecht, Gedächtnisschrift für Hans Lisken, S. 25–45, Berlin 2004, (zit.: GS-Lisken/*Kutscha/Roggan*, Seite)

Kutscha, Martin: Verdeckte „Online-Durchsuchung" und Unverletzlichkeit der Wohnung, Neue Juristische Wochenschrift 2007, S. 1169–1172, (zit.: *Kutscha*, NJW 2007, Seite)

Kutscha, Martin: Verfassungsrechtlicher Schutz des Kernbereichs privater Lebensgestaltung – nichts Neues aus Karlsruhe?, Neue Juristische Wochenschrift 2005, S. 20–22, (zit.: *Kutscha*, NJW 2005, Seite)

Lackner, Kahl / Kühl, Kristian: Strafgesetzbuch Kommentar, 29. Auflage, München 2018, (zit.: Bearbeiter in: Lackner/Kühl, §, Rn.)

Ladiges, Manuel: Unverwertbarkeit von mittels akustischer Überwachung aufgezeichneten Selbstgesprächen, Strafverteidiger 2012, S. 517–519, (zit.: *Ladiges*, StV 2012, Seite)

Lehmann, Michael / Giedke, Anna: Cloudspezifische Serververbindungen und eingesetzte Virtualisierungstechnik, Computer und Recht 2013, S. 608–616, (zit.: *Lehmann/Giedke*, CR 2013, Seite)

Lemcke, Thomas: Die Sicherstellung gem. § 94 StPO und deren Förderung durch die Inpflichtnahme Dritter als Mittel des Zugriffs auf elektronisch gespeicherte Daten, Frankfurt 1995, (zit.: *Lemcke*, Die Sicherstellung, Seite)

Lenckner, Theodor: Zur Verletzung der Vertraulichkeit des Wortes, Festschrift für Jürgen Baumann zum 70. Geburtstag, S. 135–154, Bielefeld 1992, (zit.: FS-Baumann/*Lenckner*, Seite)

Lesch, Heiko: „Hörfalle" und kein Ende – Zur Verwertbarkeit von selbstbelastenden Angaben des Beschuldigten in der Untersuchungshaft, Goltdammers Archiv 2000, S. 355–371, (zit.: *Lesch*, GA 2000, Seite)

Leupold, Andreas / Wiebe, Andreas / Glossner, Silke:Münchner Anwaltshandbuch IT-Recht, 4. Auflage, München 2021, (zit.: *Bearbeiter* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil, Rn.)

Leutheusser-Schnarrenberger, Sabine: Der Gesetzentwurf der Bundesregierung zum „großen Lauschangriff", Zeitschrift für Rechtspolitik 2005, S. 1–3, (zit.: *Leutheusser-Schnarrenberger*, ZRP 2005, Seite)

Liebig, Britta Maria:Der Zugriff auf Computerinhaltsdaten im Ermittlungsverfahren, Hamburg 2015, (zit.: *Liebig*, Der Zugriff auf Computerinhaltsdaten, Seite)

Lindemann, Michael / Reichling, Tilman:Abhören eines Selbstgesprächs, Strafverteidiger 2005, S. 650–652, (zit.: *Lindemann/Reichling*, StV 2005, Seite)

Lindemann, Michael:Der Schutz des »Kernbereichs privater Lebensgestaltung« im Strafverfahren, Juristische Rundschau 2006, S. 191–198, (zit.: *Lindemann*, JR 2006, Seite)

Lindner, Dominic / Niebler, Paul / Wenzel, Markus: Der Weg in die Cloud, 1. Auflage, Wiesbaden 2020, (zit.: *Lindner/Niebler/Wenzel*, Der Weg in die Cloud, Seite)

Löffelmann, Markus: Die Lehre von den Verwertungsverboten oder die Freude am Hindernislauf auf Umwegen, Juristische Rundschau 2009, S. 10–13, (zit.: *Löffelmann*, JR 2009, Seite)

Löffelmann, Markus: Die normativen Grenzen der Wahrheitserforschung im Strafverfahren, Berlin 2008, (zit.: *Löffelmann*, Grenzen der Wahrheitserforschung, Seite)

Löffelmann, Markus: Verwertbarkeit von Erkenntnissen aus G 10 Beschränkungsmaßnahmen, Juristische Rundschau 2019, S. 404–406, (zit.: *Löffelmann*, JR 2019, Seite)

Löffelmann, Markus:Das Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung), Zeitschrift für Internationale Strafrechtsdogmatik 2006, S. 87–98, (zit.: *Löffelmann*, ZIS 2006, Seite)

Lorenz, Frank Lucien: Absoluter Schutz versus absolute Relativität, Goltdammers Archiv 1992, S. 254–294, (zit.: *Lorenz*, GA 1992, Seite)

Luber, Stefan / Karlstetter, Florian: Beitrag „Was ist Function as a Service (FaaS)"?, cloudcomputing-insider.de vom 05.10.2018, (zuletzt abgerufen am 31.10.2021), (zit.: *Luber/Karlstetter*, Was ist Function as a Service (FaaS)?, https://www.cloudcomputing-insider.de/was-ist-function-as-a-service-faas-a-758571/)

Luch, Anika: Das neue „IT-Grundrecht" Grundbedingung einer „Online-Handlungsfreiheit", Multimedia und Recht 2011, S. 75–79, (zit.: *Luch*, MMR 2011, Seite)

Lucke, Ole-Steffen: Das Beweisverwertungsverbot von Verfassungs wegen, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2011, S. 527–531, (zit.: *Lucke*, HRRS 2011, Seite)

Lüdemann, Jörn: Die verfassungskonforme Auslegung von Gesetzen, Juristische Schulung 2004, S. 27–30, (zit.: *Lüdemann*, JuS 2004, Seite)

Mahn, Jan: Assistent unplugged – Raspi-Sprachassistent Snips ohne Cloud, Magazin für Computertechnik 2019, Heft 11, S. 34–37, (zit.: *Mahn*, c´t 2019, Heft, Seite)

Maisch, Michael Marc / Seidl, Alexander: Cloud Government: Rechtliche Herausforderungen beim Cloud Computing in der öffentlichen Verwaltung, Verwaltungsblätter für Baden-Württemberg 2012, S. 7–12, (zit.: *Maisch/Seidel*, VBlBW 2012, Seite)

Maiwald, Manfred: Zufallsfunde bei zulässiger strafprozessualer Telefonüberwachung, Juristische Schulung 1978, S. 379–385, (zit.: *Maiwald*, JuS 1979, Seite)

Malek, Klaus:Abschied von der Wahrheitssuche, Strafverteidiger 2011, S. 559–567, (zit.: *Malek*, StV 2011, Seite)

Marschall, Kevin / Herfurth, Constantin / Winter, Christian / Allwinn, Mirko: Chancen und Risiken des Einsatzes digitaler Bildforensik, Multimedia und Recht 2017, S. 152–157, (zit.: *Marschall/Herfurth/Winter/Allwinn*, MMR 2017, Seite)

Martini, Mario: Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, Juristische Arbeitsblätter 2009, S. 839–845, (zit.: *Martini*, JA 2009, Seite)

Marx, Simon:Der staatliche Zugriff auf die digitalen Sprachassistenten Alexa, Google Home und Co., Deutsches Verwaltungsblatt 2020, S. 488–494, (zit.: *Marx*, DVBl 2020, Seite)

Mather, Tim / Kumaraswamy, Subra / Latif, Shahed: Cloud Security and Privacy, Sebastopol 2009, (zit.: *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, Seite)

Mayer, Patrick Manfred: Anm. OLG Zweibrücken 1. Strafsenat, Urteil vom 18.06.2018 – 1 OLG 2 Ss 3/18, jurisPR-StrafR 19/2018 Anm. 3, (zit.: *Mayer*, jurisPR-StrafR 19/2018 Anm. 3)

Meinicke, Dirk: Big Brother und das Grundgesetz – Zulässigkeit und Grenzen der Strafprozessualen Überwachung des Surfverhaltens, DSRI-Tagungsband 2013, S. 967–981, (zit.: *Meinicke*, DSRITB 2013, Seite)

Meinicke, Dirk: Staatstrojaner, E-Mail-Beschlagnahme und Quellen-TKÜ, DSRI-Tagungsband 2012, S. 773–791, (zit.: *Meinicke*, DSRITB 2012, Seite)

Meinicke, Dirk: StPO Digital? Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, DSRI-Tagungsband 2018, S. 835–857, (zit.: *Meinicke*, DSRITB 2018, Seite)

Meininghaus, Florian: Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, Hamburg 2007, (zit.: *Meininghaus*, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, Seite)

Meixner, Robin: Das Widerspruchserfordernis des BGH bei Beweisverwertungsverboten, Heidelberg 2014, (zit.: *Meixner*, Das Widerspruchserfordernis, Seite)

Mell, Peter / Grace, Timothy: The NIST Definition of Cloud-Computing – The NIST Definition of Cloud-Computing, abrufbar über: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (zuletzt abgerufen am 31.10.2021), (zit.: *Mell/Grace*, The NIST Definition of Cloud-Computing, Seite)

Mende, Boris: Grenzen privater Ermittlungen durch den Verletzten einer Straftat, Berlin 2001, (zit.: *Mende*, Grenzen privater Ermittlungen, Seite)

Merten, Detlef / Papier, Hans-Jürgen (Hrsg.): Handbuch der Grundrechte, Band II, Heidelberg 2006, (zit.: *Bearbeiter* in: Handbuch der Grundrechte, §, Rn.)

Merten, Detlef / Papier, Hans-Jürgen (Hrsg.): Handbuch der Grundrechte, Band V, Heidelberg 2013, (zit.: *Bearbeiter* in: Handbuch der Grundrechte, §, Rn.)

Metz, Jochen: Verwertbarkeit von tätereigenen Tatvideos, Neue Zeitschrift für Strafrecht 2020, S. 9–11, (zit.: *Metz*, NStZ 2020, Seite)

Meurer, Dieter: Anm. zu BGH Urteil v. 17.2.1989 – 2 StR 402, Juristische Rundschau 1990, S. 389–392, (zit.: *Meurer*, JR 1990, Seite)

Meyer-Goßner, Lutz / Schmitt, Bertram: Strafprozessordnung, 64. Auflage, München 2021, (zit.: *Bearbeiter* in: Meyer-Goßner/Schmitt, §, Rn.)

Meyer-Mews, Hans: Beweisverwertungsverbote im Strafverfahren, Juristische Schulung 2004, S. 126–130, (zit.: *Meyer-Mews*, JuS 2004, Seite)

Meyer-Mews, Hans: Hände weg von den verbotenen Früchten – Fernwirkung im Strafverfahrensrecht, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2015, S. 398–406, (zit.: *Meyer-Mews*, HRRS 2015, Seite)

Meyer-Wieck, Hannes: Der große Lauschangriff, Freiburg 2005, (zit.: *Meyer-Wieck*, Der große Lauschangriff, Seite)

Michalke, Regina: Staatlicher Zugriff auf elektronische Medien, Strafverteidigerforum 2008, S. 287–292, (zit.: *Michalke*, StraFo 2008, Seite)

Miftari, Duresa / Henrichs, Katrin:Alexa & Co. – Sprachassistenzsysteme als neuer polizeilicher Ermittlungsansatz?, Zwischen innovativer Polizeiarbeit und neuem Management, S. 297–319, Baden-Baden 2020, (zit.: *Miftari/Henrichs*, Zwischen innovativer Polizeiarbeit und neuem Managements, Seite)

Mitsch, Wolfgang: Strafprozessual unantastbare „Kommunikation mit sich selbst", Neue Juristische Wochenschrift 2012, S. 1486–1488, (zit.: *Mitsch*, NJW 2012, Seite)

Moll, Ricarda / Rusch-Rodosthenous, Miriam: Amazon Alexa – Wann ist der Sprachassistent ganz Ohr: Ein Reaktionscheck, Düsseldorf 2017, abgerufen unter: https://www.vzbv.de/sites/default/files/downloads/2020/01/24/kurzbericht_alexa_sprach erkennung.pdf (zuletzt abgerufen am 31.10.2021), (zit.: *Moll/Rusch-Rodosthenous*, Amazon Alexa – ein Reaktionscheck, Seite)

Momsen, Carsten / Hercher, Nils: Digitale Beweismittel im Strafprozess – Eignung, Gewinnung, Verwertung und Revisibilität Beitrag zum 37. Strafverteidigertag, Freiburg 2013, S. 173 – 196, abgerufen unter: http://strafverteidigervereinigungen.de/Material/Themen/Technik%20&%20Ueberwachung/37_momsen.pdf (zuletzt abgerufen am 31.10.2021), (zit.: *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, Seite)

Momsen, Carsten: Digitale Beweismittel aus Sicht der Strafverteidigung, Cybercrime und Cyberinvestigations, S. 67–91, Baden-Baden 2015, (zit.: *Momsen*, Cybercrime und Cyberinvestigations, Seite)

Momsen, Carsten: Entsperrung biometrischer Sicherungen im Strafverfahren, Deutsche Richterzeitung 2018, S. 140–143, (zit.: *Momsen*, DRiZ 2018, Seite)

Momsen, Carsten: Zum Umgang mit digitalen Beweismitteln im Strafprozess, Festschrift für Werner Beulke zum 70. Geburtstag, S. 871–887, Heidelberg 2015, (zit.: FS-Beulke/*Bearbeiter*, Seite)

Morlok, Michael: Grundrechte, 6. Auflage, Baden-Baden 2017, (zit.: *Morlok*, Grundrechte, Rn.)

Mosbacher, Andreas:Verwertungsverbot bei Durchsuchungsanordnung des Staatsanwalts, Neue Juristische Wochenschrift 2007, S. 3686–3688, (zit.: *Mosbacher*, NJW 2007, Seite)

Müller, Daniel: Cloud Computing – Strafrechtlicher Schutz privater und geschäftlicher Nutzerdaten vor Innentäter Angriffen de lege lata und de lege ferenda, Berlin 2020, (zit.: *Müller*, Cloud Computing, Seite)

Müller, Marion: Nachfrage nach Sprachassistenten nimmt zu, Aktiengesellschaft 2020, S. R270, (zit.: *Müller*, AG 2020, Seite)

Müller, Sebastian:Internetermittlungen und der Umgang mit digitalen Beweismitteln im (Wirtschafts-)Strafverfahren, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 2020, S. 96–101, (zit.: *Müller*, NZWiSt 2020, Seite)

Müssig, Bernd: Beweisverbote im Legitimationszusammenhang von Strafrechtstheorie und Strafverfahren, Goltdammers Archiv 1999, S. 119–142, (zit.: *Müssig*, GA 1999, Seite)

Muthorst, Olaf: Das heimlich aufgezeichnete Selbstgespräch im Strafverfahren -Anmerkung zum BGH Urteil vom 22.12.2011 – 2 StR509/1, Studentische Zeitschrift für Rechtswissenschaft 2013, S. 169–179, (zit.: *Muthorst*, StudZR 2013, Seite)

Nachbaur, Andreas: Standortfeststellung und Art. 10 GG – Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers", Neue Juristische Wochenschrift 2007, S. 335–337, (zit.: *Nachbaur*, NJW 2007, Seite)

Nack, Armin: Akustische Wohnraumüberwachung und Verwertungsverbot, Festschrift für Kay Nehm zum 65. Geburtstag, S. 310–325, Berlin 2006, (zit.: FS-Nehm/*Nack*, Seite)

Nack, Armin:Verwertung rechtswidriger Ermittlungen nur zugunsten des Beschuldigten?, Strafverteidiger Forum 1998, S. 366–374, (zit.: *Nack*, StraFo 1998, Seite)

Nägele, Thomas / Jacobs, Sven: Rechtsfragen des Cloud-Computings, Zeitschrift für Urheber- und Medienrecht 2010, S. 281–292, (zit.: *Nägele/Jacobs*, ZUM 2010, Seite)

Neubacher, Frank: Kriminologie, 4. Auflage, Baden-Baden 2020, (zit.: *Neubacher*, Kriminologie, §, Rn.)

Neuber, Florian: Beweisverwertungsverbote im Strafprozess: Rechtsstaatlichkeitsanforderungen an die Abwägungslehre: Ein methodischer Vorschlag zur Konturierung der Abwägung, Münster 2017, (zit.: *Neuber*, Beweisverwertungsverbote im Strafprozess, Seite)

Neuber, Florian: Unselbstständige Beweisverwertungsverbote im Strafprozess -Die Abwägungslehre auf dem methodischen Prüfstand, Neue Zeitschrift für Strafrecht 2019, S. 113–123, (zit.: *Neuber*, NStZ 2019, Seite)

Neuhaus, Melanie: Die Auswertung von Smartphones im Ermittlungsverfahren, Strafverteidiger 2020, S. 489–492, (zit.: *Neuhaus*, StV 2020, Seite)

Neuhaus, Ralf: Zur Fernwirkung von Beweisverwertungsverboten, Neue Juristische Wochenschrift 1990, S. 1221–1222, (zit.: *Neuhaus*, NJW 1990, Seite)

Neuhöfer, Daniel: Soziale Netzwerke: Private Nachrichteninhalte im Strafverfahren, Juristische Rundschau 2015, S. 21–31, (zit.: *Neuhöfer*, JR 2015, Seite)

Neumann, Linus / Kurz, Constanze / Rieger, Felix:Sachverständigenauskunft zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Ausschussdrucksache 18/11272), Mai 2017, abrufbar unter: https://www.ccc.de/system/uploads/227/original/Stellungnahme_CCC-Staatstrojaner.pdf, (zuletzt abgerufen am 31.10.2021) (zit.: *Chaos Computerclub*, Stellungnahme, Seite)

Nicolai, Florian: Der Zugriff auf beim Provider (endgespeicherte) E-Mails, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2021, S. 365–368, (zit.: *Nicolai*, HRRS 2021, Seite)

Niehaus, Holger: Geschwindigkeitsüberwachung durch Videoaufzeichnung, Deutsches Autorrecht 2009, S. 632–637, (zit.: *Niehaus*, DAR 2009, Seite)

Niehaus, Holger: Verwertbarkeit von Dashcam-Aufzeichnungen im Straf- und Ordnungswidrigkeitenverfahren, Neue Zeitschrift für Verkehrsrecht 2016, S. 551–556, (zit.: *Niehaus*, NZV 2016, Seite)

Niemann, Fabian / Hennrich, Thorsten: Kontrolle in den Wolken? Auftragsdatenverarbeitung in Zeiten des Cloud-Computing, Computer und Recht 2010, S. 686–692, (zit.: *Niemann/Hennrich*, CR 2010, Seite)

Niemann, Fabian / Paul, Jörg-Alexander: Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings, Kommunikation und Recht 2009, S. 444–452, (zit.: *Niemann/Paul*, K&R 2009, Seite)

Niemann, Fabian / Paul, Jörg-Alexander: Rechtsfragen des Cloud Computing, Berlin 2014, (zit.: *Bearbeiter* in: Niemann/Paul, Praxishandbuch Rechtsfragen des Cloud Computing, Seite, Rn.)

Nöding, Toralf: Die Novellierung der strafprozessualen Regelungen zur Telefonüberwachung, Strafverteidiger Forum 2007, S. 456–463, (zit.: *Nöding*, StraFo 2007, Seite)

Nüse, Karl-Heinz: Zu den Beweisverboten im Strafprozess, Juristische Rundschau 1966, S. 281–288, (zit.: *Nüse*, JR 1966, Seite)

Oberhaus, Nils: Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, Neue Juristische Wochenschrift 2010, S. 651–655, (zit.: *Oberhaus*, NJW 2010, Seite)

Osmer, Jan-Dierk: Der Umfang des Beweisverwertungsverbotes nach § 136a StPO, Hamburg 1966, (zit.: *Osmer*, Umfang des Beweisverwertungsverbotes, Seite)

Ostendorf, Heribert: Strafprozessrecht, 3. Auflage, Baden-Baden 2018, (zit.: *Ostendorf*, Strafprozessrecht, Rn.)

Otto, Harro: Die strafprozessuale Verwertbarkeit von Beweismitteln, die durch Eingriff in Rechte anderer von Privaten erlangt wurden, Festschrift für Theodor Kleinknecht zum 75. Geburtstag, S. 319–340, München 1985, (zit.: FS-Kleinknecht/*Otto*, Seite)

Otto, Harro: Grenzen und Tragweite der Beweisverbote im Strafverfahren, Goltdammers Archiv 1970, S. 289–305, (zit.: *Otto*, GA 1970, Seite)

Paa, Bernhard: Der Zugriff der Strafverfolgungsbehörden auf das Private im Kampf gegen schwere Kriminalität, Heidelberg 2013, (zit.: *Paa*, Der Zugriff der Strafverfolgungsbehörden auf das Private, Seite)

Park, Thilo: Durchsuchung und Beschlagnahme, 4. Auflage, München 2018, (zit.: *Park*, Durchsuchung und Beschlagnahme, Rn.)

Paschke, Marian / Berlit, Wolfgang / Meyer, Claus (Hrsg): Hamburger Kommentar Gesamtes Medienrecht, 4. Auflage, Baden-Baden 2021, (zit. *Bearbeiter* in: HH-Ko/MedienR, Abschnitt, Rn.)

Paul, Tobias:Unselbständige Beweisverwertungsverbote in der Rechtsprechung, Zeitschrift für Strafrecht 2013, S. 489–497, (zit.: *Paul*, NStZ 2013, Seite)

Paulsen, Monrad: Grundzüge des amerikanischen Strafprozesses, Zeitschrift für gesamte Strafrechtswissenschaft 1965, S. 637–668, (zit.: *Paulsen*, ZStW 1965, Seite)

Pelz, Christian: Beweisverwertungsverbote und hypothetische Ermittlungsverläufe, München 1993, (zit.: *Pelz*, Beweisverwertungsverbote und hypothetische Ermittlungsverläufe, Seite)

Peres, Holger: Strafprozessuale Beweisverbote und Beweisverwertungsverbote, München 1991, (zit.: *Peres*, Strafprozessuale Beweisverbote und Beweisverwertungsverbote, Seite)

Peters, Kristina: Anwesenheitsrechte bei der Durchsicht gemäß § 110 StPO: Bekämpfung der Risiken und Nebenwirkungen einer übermächtigen Ermittlungsmaßnahme, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 2017, S. 465–472, (zit.: *Peters*, NZWiSt 2017, Seite)

Pieper, Niels: Grundstrukturen des verfassungsrechtlichen Datenschutzes – Zum Schutz personenbezogener Daten durch die Grundrechte des Grundgesetzes bei Maßnahmen der Gefahrenabwehr, Juristische Arbeitsblätter 2018, S. 598–605, (zit.: *Pieper*, JA 2018, Seite)

Pohle, Jan / Ammann, Thorsten: Über den Wolken... – Chancen und Risiken des Cloud Computing, Computer und Recht 2009, S. 273–278, (zit.: *Pohle/Ammann*, CR 2009, Seite)

Popp, Andreas: Die „Staatstrojaner"-Affäre: (Auch) ein Thema für den Datenschutz – Kurzer Überblick aus strafprozessualer und datenschutzrechtlicher Sicht, Zeitschrift für Datenschutz 2012, S. 51–55, (zit.: *Popp*, ZD 2012, Seite)

Poscher, Ralf:Menschenwürde und Kernbereichsschutz, Juristenzeitung 2009, S. 269–277, (zit.: *Poscher*, JZ 2009, Seite)

Pötters, Stephan / Werkmeister, Christoph: Der verfassungsrechtliche Konflikt zwischen Freiheit und Sicherheit im Zeitalter des Internets, Juristische Ausbildung 2013, S. 5–12, (zit.: *Pötters/Werkmeister*, JURA 2013, Seite)

Prittwitz, Cornelius: Zur Verwertbarkeit zufällig aufgezeichneter Raum- und Hintergrundgespräche, Strafverteidiger 2009, S. 437–442, (zit.: *Prittwitz*, StV 2009, Seite)

Puschke, Jens / Singelnstein, Tobias: Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1. 1. 2008, Neue Juristische Wochenschrift 2008, S. 113–119, (zit.: *Puschke/Singelnstein*, NJW 2008, Seite)

Radtke, Henning / Hohmann, Olaf: Strafprozessordnung Kommentar, 1. Auflage, München 2011, (zit.: *Bearbeiter* in: Radtke/Hohmann, §, Rn.)

Rammos, Thanos / von Rosen, Johannes: Urheberrechtliche Fragen beim Einsatz von Sprachassistenten mit Vorlesefunktion, Zeitschrift für Urheber- und Medienrecht 2020, S. 25–31, (zit.: *Rammos/von Rosen*, ZUM 2020, Seite)

Ranft, Otfried: Bemerkungen zu den Beweisverboten im Strafprozeß, Festschrift für Günter Spendel zum 70. Geburtstag, S. 719–736, Berlin 1992, (zit.: FS-Spendel/*Ranft*, Seite)

Ransiek, Andreas: Durchsuchung, Beschlagnahme und Verwertungsverbot, Strafverteidiger 2002, S. 565–571, (zit.: *Ransiek*, StV 2002, Seite)

Ransiek, Andreas: Rechtswidrige Ermittlungen und die Fernwirkung von Beweisverwertungsverboten, Festschrift für Werner Beulke zum 70. Geburtstag, S. 949–961, Heidelberg 2015, (zit.: FS-Beulke/*Ransiek*, Seite)

Reeb, Philipp:Internal Investigations, Berlin 2011, (zit.: *Reeb*, Internal Investigations, Seite)

Rehbein, Mareike: Die Verwertbarkeit von nachrichtendienstlichen Erkenntnissen aus dem In und Ausland im deutschen Strafprozess, Berlin 2011, (zit.: *Rehbein*, Verwertbarkeit von nachrichtendienstlichen Erkenntnissen, Seite)

Reichert, Johannes: Der Schutz des Kernbereichs privater Lebensgestaltung in den Polizeigesetzen des Bundes und der Länder, Tübingen 2015, (zit.: *Reichert*, Der Schutz des Kernbereichs, Seite)

Reichert-Hammer, Hansjörg: Zur Fernwirkung von Beweisverwertungsverboten, Juristische Schulung 1989, S. 446–500, (zit.: *Reichert-Hammer*, JuS 1989, Seite)

Reinecke, Jan: Die Fernwirkung von Beweisverwertungsverboten, München 1990, (zit.: *Reinecke*, Fernwirkung von Beweisverwertungsverboten, Seite)

Reinheimer, Stefan: Cloud Computing – Die Infrastruktur der Digitalisierung, Berlin 2018, (zit.: *Bearbeiter* in: Reinheimer Cloud-Computing, Seite)

Reiß, Marc: Der strafprozessuale Schutz verfassungsrechtlich geschützter Strafverteidiger 2008, S. 539–548, (zit.: *Reiß*, StV 2008, Seite)

Renka, Susanne: Zur Verwertbarkeit von Selbstkommunikation im deutschen Strafprozess, Frankfurt 2016, (zit.: *Renka*, Verwertbarkeit von Selbstkommunikation, Seite)

Riegel, Reinhard: Das Dirnhofer Urteil des Bundesgerichtshofs und seine Konsequenzen für die Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden, Juristenzeitung 1980, S. 757–759, (zit.: *Riegel*, JZ 1980, Seite)

Rieß, Peter: Subsidiaritätsverhältnisse und Subsidiaritätsklauseln im Strafverfahren, Gedächtnisschrift für Karlheinz Meyer, S. 367–390, Berlin 1990, (zit.: GS-Meyer/*Rieß*, Seite)

Rieß, Peter: Über die Aufgaben des Strafverfahrens, Juristische Rundschau 2006, S. 269–277, (zit.: *Rieß*, JR 2006, Seite)

Rissing-van Saan, Ruth / Grünewald, Anette / Kröger, Perdita / Krüger, Matthias (Hrsg.): Leipziger Kommentar StGB, Band 6, §§ 146–210 StGB, 12. Auflage, Berlin 2018, (*Bearbeiter* in: LK-StGB, §, Rn.)

Rogall, Klaus: Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus, Juristenzeitung 2008, S. 818–830, (zit.: *Rogall*, JZ 2008, Seite)

Rogall, Klaus: Dogmatische Grundlagen der Verwertungsverbote, Strafverteidiger 1996, S. 513–519, (zit.: *Rogall*, StV 1996, Seite)

Rogall, Klaus: Hypothetische Ermittlungsverläufe im Strafprozeß – Ein Beitrag zur Lehre der Beweiserhebungs- und Beweisverwertungsverbote, Neue Zeitschrift für Strafrecht 1988, S. 385–393, (zit.: *Rogall*, NStZ 1988, Seite)

Rogall, Klaus: Informationseingriff und Gesetzesvorbehalt im Strafprozess, Berlin 1992, (zit.: *Rogall*, Informationseingriff und Gesetzesvorbehalt, Seite)

Rogall, Klaus: Kernbereichssystematik im Strafverfahren, Festschrift für Gerhard Fezer zum 70. Geburtstag, S. 61–86, Berlin 2008, (zit.: FS-Fezer/*Bearbeiter*, Seite)

*Rogall, Klaus:*Gegenwärtiger Stand und Entwicklungstendenzen der Lehre von den strafprozessualen Beweisverboten, Zeitschrift für gesamte Strafrechtswissenschaft 1979, S. 1–44, (zit.: *Rogall*, ZStW 1979, Seite)

Roggan, Fredrik: Der Schutz des Kernbereichs privater Lebensgestaltung bei strafprozessualer Telekommunikationsüberwachung, Strafverteidiger 2011, S. 762–766, (zit.: *Roggan*, StV 2011, Seite)

Roggan, Fredrik: Die „Technikoffenheit" von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen – Die Problematik der Auslegung von Gesetzen über ihren Wortlaut oder Wortsinn hinaus, Neue Juristische Wochenschrift 2015, S. 1995–1999, (zit.: *Roggan*, NJW 2015, Seite)

Roggan, Fredrik: Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung, Strafverteidiger 2017, S. 821–829, (zit.: *Roggan*, StV 2017, Seite)

Roggan, Fredrik: Moderne Telekommunikationsüberwachung: Eine kritische Bestandsaufnahme, Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 2003, S. 76–95, (zit.: *Roggan*, KritV 2003, Seite)

Rottmeier, Christian / Eckel, Philipp: Die Entschlüsselung biometrisch gesicherter Daten im Strafverfahren, Neue Zeitschrift für Strafrecht 2020, S. 193–200, (zit.: *Rottmeier/Eckel*, NStZ 2020, Seite)

*Rottmeier, Christian:*Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, Tübingen 2017, (zit.: *Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, Seite)

Roxin, Claus / Schäfer, Gerhard / Widmaier, Gunter: Die Mühlenteichtheorie, Strafverteidiger 2006, S. 655–661, (zit.: Roxin//Schäfer/Widmaier, StV 2006, Seite)

Roxin, Claus / Schäfer, Gerhard / Widmaier, Gunter: Die Mühlenteichtheorie – Überlegungen zur Ambivalenz von Verwertungsverboten, Festschrift zu Ehren des Strafrechtsausschusses der Bundesrechtsanwaltskammer, S. 435–446, Münster 2006, (zit.: FS-Strauda/*Roxin/Schäfer/Widmaier*, Seite)

Roxin, Claus / Schünemann, Bernd:Strafverfahrensrecht, 29. Auflage, München 2017, (zit.: *Roxin/Schünemann*, Strafverfahrensrecht, §, Rn.)

Roxin, Claus: Aushorchungen in der Untersuchungshaft als Überführungsmittel, Festschrift für Klaus Geppert zum 70. Geburtstag, S. 549–567, Berlin 2011, (zit.: FS-Geppert/*Roxin*, Seite)

Roxin, Claus: Die Rechtsprechung des Bundesgerichtshofs zum Strafverfahrensrecht – ein Rückblick auf 40 Jahre, 40 Jahre Bundesgerichtshof, S. 66–99, (zit.: *Roxin* in: Jauernig/Roxin Die Rechtsprechung des BGH, Seite)

Roxin, Claus: Großer Lauschangriff und Kernbereich privater Lebensgestaltung, Festschrift für Reinhard Böttcher zum 70. Geburtstag, S. 159–174, Berlin 2007, (zit.: FS-Böttcher/*Roxin*, Seite)

Roxin, Claus: Kernbereichsschutz und Straftatermittlung, Festschrift für Jürgen Wolter zum 70. Geburtstag, S. 1057–1076, Berlin 2013, (zit.: FS-Wolter/*Roxin*, Seite)

Roxin, Claus: Zum Beweisverwertungsverbot bei bewusster Missachtung des Richtervorbehalts nach § 105 I 1 StPO, Neue Zeitschrift für Strafrecht 2007, S. 616–618, (zit.: Roxin, NStZ 2007, Seite)

*Roxin, Claus:*Anm. zu BGH, Urteil vom 15. 2. 1989 – 2 StR 402/88 (LG Fulda), Neue Zeitschrift für Strafrecht 1989, S. 376–379, (zit.: *Roxin*, NStZ 1989, Seite)

Rudolphi, Hans-Joachim: Die Revisibilität von Verfahrensmängeln im Strafprozess, Monatsschrift für Deutsches Recht 1970, S. 93–100, (zit.: *Rudolphi*, MDR 1970, Seite)

Rüscher, Daniel: Alexa, Siri und Google als digitale Spione im Auftrag der Ermittlungsbehörden, Neue Zeitschrift für Strafrecht 2018, S. 687–692, (zit.: *Rüscher*, NStZ 2018, Seite)

Ruthig, Josef:Die Unverletzlichkeit der Wohnung, Juristische Schulung 1998, S. 506–516, (zit.: *Ruthig*, JuS 1998, Seite)

Rux, Johannes: Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, Juristenzeitung 2007, S. 285–295, (zit.: *Rux*, JZ 2007, Seite)

Sachs, Michael (Hrsg.): Grundgesetz Kommentar, 9. Auflage, München 2021, (zit.: *Bearbeiter* in: Sachs-GG, Art., Rn.)

Sachs, Michael / Krings, Thomas: Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Juristische Schulung 2008, S. 481–486, (zit.: *Sachs/Krings*, JuS 2008, Seite)

Sankol, Barry: Die Qual der Wahl: § 113 TKG oder §§ 100g, 100h StPO? Die Kontroverse über das Auskunftsverlangen von Ermittlungsbehörden gegen Access-Provider bei dynamischen IP-Adressen, Multimedia und Recht 2006, S. 361–365, (zit.: *Sankol*, MMR 2006, Seite)

Satzger, Helmut / Schluckebier, Wilhelm / Widmaier, Gunter (Hrsg.): Strafprozessordnung – Kommentar, 4. Auflage, Köln 2020, (zit.: *Bearbeiter* in: SSW-StPO, §, Rn.)

Schaar, Peter / Landwehr, Sebastian: Anm. zum Beschluss des BGH vom 31. 1. 2007 – StB 18/06 – zur verdeckten Online-Durchsuchung, Kommunikation & Recht 2007, S. 203–205, (zit.: *Schaar/Landwehr*, K&R 2007, Seite)

Schaar, Peter:Große Koalition, wenig Datenschutz?, Multimedia und Recht 2018, S. 125–126, (zit.: *Schaar*, MMR 2018, Seite)

Schäfer, Helmut: Der Computer im Strafverfahren, Zeitschrift für Wirtschafts- und Steuerstrafrecht 1989, S. 8–13, (zit.: *Schäfer*, wistra 1989, Seite)

Schelzke, Ricarda Christine:Die iCloud als Gefahr für den Rechtsanwalt?, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2013, S. 86–91, (zit.: *Schelzke*, HRRS 2013, Seite)

Schenke, Ralf: Präventive Überwachung der Telekommunikation, Archiv des öffentlichen Rechts 2000, S. 1–44, (zit.: *Schenke*, AöR 2000, Seite)

Scheurle, Klaus-Dieter / Mayen, Thomas (Hrsg.): Telekommunikationsgesetz Kommentar, 3. Auflage, München 2018, (zit.: *Bearbeiter* in: Scheurle/Mayen-TKG, §, Rn.)

Schlegel, Stephan: Beschlagnahme von E-Mail-Verkehr beim Provider, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 2007, S. 44–51, (zit.: *Schlegel*, HRRS 2007, Seite)

Schlegel, Stephan: Warum die Festplatte keine Wohnung ist – Art. 13 GG und die „Online-Durchsuchung", Goltdammers Archiv 2007, S. 648–663, (zit.: *Schlegel*, GA 2007, Seite)

Schlüchter, Ellen: Anm. zu BGH Urteil v. 24.8.1983 — 3 StR 136/83, Juristische Rundschau 1984, S. 517–522, (zit.: *Schlüchter*, JR 1984, Seite)

Schmid, Daniel: Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen, Berlin 2017, (zit.: *Schmid*, Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen, Seite)

Schmidl, Michael: IT-Recht von A-Z, 2. Auflage, München 2014, (zit.: *Schmidl*, IT-Recht, Seite)

Schmidt-Bens, Johanna: Cloud Computing Technologien und Datenschutz, Edewecht 2012, (zit.: *Schmidt-Bens*, Cloud Computing Technologien und Datenschutz, Seite)

Schmidt-Leichner, Erich: Diskussion, Verhandlungen des 46. Deutschen Juristentages, Band II: Diskussion, Teil F, F 137-F140, München 1966, (zit.: *Schmidt-Leichner*, 46. DJT, Bd. 2, Seite)

Schmitt, Rudolf: Tonbänder im Strafprozess, Juristische Schulung 1967, S. 19–25, (zit.: *Schmitt*, JuS 1967, Seite)

Schnabel, Christoph:Anm. zu BVerfG, Beschluss des Ersten Senats vom 24. Januar 2012- 1 BvR 1299/05, Computer und Recht 2012, S. 253–255, (zit.: *Schnabel*, CR 2012, Seite)

Schnarr, Karl Heinz: Zur Verknüpfung von Richtervorbehalt, staatsanwaltschaftlicher Eilanordnung und richterlicher Bestätigung, Neue Zeitschrift für Strafrecht 1991, S. 209–216, (zit.: Schnarr, NStZ 1991, Seite)

Schneider, Hartmut: Anm. zum BGH Urteil v. 17.2.2016 – 2 StR 25/15, Neue Zeitschrift für Strafrecht 2016, S. 553–557, (zit.: *Schneider*, NStZ 2016, Seite)

Schneider, Hartmut: Verdeckte Ermittlungen in Haftanstalten, Neue Zeitschrift für Strafrecht 2001, S. 8–15, (zit.: *Schneider*, NStZ 2001, Seite)

Schneider, Hartmut: Zur Berücksichtigung hypothetischer Ermittlungsverläufe in Fällen grob fehlerhafter Annahme von Gefahr im Verzug bei Wohnungsdurchsuchungen, Neue Zeitschrift für Strafrecht – Sonderheft 2009, S. 46–52, (zit.: *Schneider*, NStZ – Sonderheft 2009, Seite)

Schoch, Friedrich: Der verfassungsrechtliche Schutz des Fernmeldegeheimnisses (Art. 10 GG), Juristische Ausbildung 2011, S. 194–204, (zit.: *Schoch*, Jura 2011, Seite)

Schönke, Adolf / Schröder, Horst: Strafgesetzbuch Kommentar, 30. Auflage, München 2019, (zit.: *Bearbeiter* in: Schönke/Schröder, §, Rn.)

Schröder, Christian / Haag, Nils Christian: Neue Anforderungen an Cloud Computing für die Praxis, Zeitschrift für Datenschutz 2011, S. 147–152, (zit.: *Schröder/Haag*, ZD 2011, Seite)

Schröder, Svenja: Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung im Strafprozess, Berlin 1992, (zit.: *Schröder*, Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung, Seite)

Schroeder, Friedrich-Christian / Verrel, Torsten: Strafprozessrecht, 7. Auflage, München 2017, (zit.: *Schroeder/Verrel*, Strafprozessrecht, §, Rn.)

Schroeder, Friedrich-Christian: Die Ermittlung des Aufenthaltsortes des Beschuldigten als Anwendungsvoraussetzung strafprozessualer Zwangsmaßnahmen, Goltdammers Archiv 2005, S. 73–80, (zit.: *Schroeder*, GA 2005, Seite)

Schroth, Ulrich: Beweisverwertungsverbote im Strafverfahren – Überblick, Strukturen und Thesen zu einem umstrittenen Thema, Juristische Schulung 1998, S. 969–980, (zit.: *Schroth*, JuS 1998, Seite)

Schult, Stefanie: Plattformregulierung im Audiobereich – Mittendrin statt nur dabei?, Multimedia und Recht 2020, S. 448–452, (zit.: *Schult*, MMR 2020, Seite)

Schuster, Fabian / Reichl, Wolfgang: Cloud Computing & Saas: Was sind die wirklich neuen Fragen?, Computer und Recht 2010, S. 38–43, (zit.: *Schuster/Reichl*, CR 2010, Seite)

Schwaben, Sylvia: Die personelle Reichweite von Beweisverwertungsverboten, Göttingen 2005, (zit.: *Schwaben*, personelle Reichweite von Beweisverwertungsverboten, Seite)

Schwabenbauer, Thomas: Heimliche Grundrechtseingriffe, Tübingen 2013, (zit.: *Schwabenbauer*, Heimliche Grundrechtseingriffe, Seite)

Schwabenbauer, Thomas: Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter, Archiv für Öffentliches Recht 2012, S. 1–41, (zit.: *Schwabenbauer*, AöR 2012, Seite)

Seebode, Manfred: Anm. zu BGH Urteil v. 28.04.1987 – 5 StR 666/86, Juristische Rundschau 1988, S. 427–432, (*Seebode*, JR 1988, Seite)

Seifert, Jens: Problemkreis des Grundrechtsverzichts, Juristische Ausbildung 2007, S. 99–104, (zit.: *Seifert*, Jura 2007, Seite)

Seitz, Nicolai:Strafverfolgungsmaßnahmen im Internet, Köln 2004, (zit.: *Seitz*, Strafverfolgungsmaßnahmen im Internet, Seite)

Sieber, Ulrich: Straftaten und Strafverfolgung im Internet, Verhandlungen des 69. Deutschen Juristentages, Band I: Gutachten / Teil C, München 2012, (zit.: *Sieber*, Verhandlungen des 69. Deutschen Juristentages, Seite)

Sievers, Marc:Der Schutz der Kommunikation im Internet durch Artikel des 10 des Grundgesetzes, Kiel 2002, (zit.: *Sievers*, Der Schutz der Kommunikation im Internet, Seite)

Singelnstein, Tobias / Derin, Benjamin: Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens – Was aus der StPO-Reform geworden ist, Neue Juristische Wochenschrift 2017, S. 2646–2652, (zit.: *Singelnstein/Derin*, NJW 2017, Seite)

Singelnstein, Tobias / Putzer, Max:Rechtliche Grenzen strafprozessualer Ermittlungsmaßnahmen – Aktuelle Bestandsaufnahme und neue Herausforderungen, Goltdammers Archiv 2015, S. 564–578, (zit.: *Singelnstein/Putzer*, GA 2015, Seite)

Singelnstein, Tobias: Big Data und Strafverfolgung, Big Data – Regulative Herausforderungen, S. 179–185, (zit.: *Singelnstein* in: Big Data – Regulative Herausforderungen, Seite)

Singelnstein, Tobias:Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, Neue Zeitschrift für Strafrecht 2012, S. 593–605, (zit.: *Singelnstein*, NStZ 2012, Seite)

Sinn, Arndt: Stellungnahme zum Entwurf der BT-Drucksache 18/11272 sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18(6)334), Osnabrück 2017, abrufbar unter: https://www.bundestag.de/resource/blob/509050/6f72dd42df72be6f2da6a024475b3f8a/sinn-data.pdf (zuletzt abgerufen am 31.10.2021), (zit.: *Sinn*, Stellungnahme zum Entwurf der BT-Drucksache 18/11272, Seite)

Skistims, Hendrik / Roßnagel, Alexander: Rechtlicher Schutz vor Staatstrojanern? Verfassungsrechtliche Analyse einer Regierungs-Malware, Zeitschrift für Datenschutz 2012, S. 3–7, (zit.: *Skistims/Roßnagel*, ZD 2012, Seite)

Slyzik, Andreas: Schmerzensgeld Handbuch, 16. Auflage, München 2020, (zit.: *Bearbeiter* in: Slyzik, Handbuch Schmerzensgeld, Rn.)

Sodan, Helge (Hrsg.):Sodan Grundgesetz, 4. Auflage, München 2018, (zit.: *Bearbeiter* in: Sodan-GG, Art., Rn.)

Soiné, Michael: Die strafprozessuale Online-Durchsuchung, Neue Zeitschrift für Strafrecht 2018, S. 497–504, (zit.: *Soiné*, NStZ 2018, Seite)

Soiné, Michael: Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder, Neue Zeitschrift für Verwaltungsrecht 2012, S. 1585–1589, (zit.: *Soiné*, NVwZ 2012, Seite)

Soiné, Michael: Identifizierung von E-Mails mit Schadprogrammen durch Sicherheitsbehörden – Grundrechtsfragen bei der Auslegung des „entwicklungsoffenen" Fernmeldegeheimnisses, Multimedia und Recht 2015, S. 22–25, (zit.: *Soiné*, MMR 2015, Seite)

Son, Jae-Young: Heimliche Polizeieingriffe in das informationelle Selbstbestimmungsrecht, Berlin 2006, (zit.: *Son*, Heimliche Polizeieingriffe, Seite)

Spatscheck, Rainer: Beschlagnahme von Computerdaten und E-Mails beim Berater, Festschrift für Rainer Hamm zum 65. Geburtstag, S. 733–749, (zit.: FS-Hamm/*Spatscheck*, Seite)

Spendel, Günter: Beweisverbote im Strafprozess, Neue Juristische Wochenschrift 1966, S. 1102–1108, (zit.: *Spendel*, NJW 1966, Seite)

Stadler, Thomas: Zulässigkeit der heimlichen Installation von Überwachungssoftware Trennung von Online-Durchsuchung und Quellen-Telekommunikationsüberwachung möglich? Multimedia und Recht 2012, S. 18–20, (zit.: *Stadler*, MMR 2012, Seite)

Starck, Christian: Das neue Recht polizeilicher Datenerhebung und -verarbeitung in Niedersachsen, Niedersächsische Verwaltungsblätter 2008, S. 145–152, (zit.: *Starck*, NdsVbl 2008, Seite)

Stein, Ekkehart / Frank, Götz: Staatsrecht, 21. Auflage, Tübingen 2010, (zit.: *Stein/Frank*, Staatsrecht, Seite)

Stoffer, Hannah: Wie viel Privatisierung „verträgt" das strafprozessuale Ermittlungsverfahren, Tübingen 2016, (zit.: *Stoffer*, Privatisierung des strafprozessualen Ermittlungsverfahren, Seite)

Störmer, Rainer: Dogmatische Grundlagen der Verwertungsverbote, Marburg 1992, (*Störmer*, Grundlagen der Verwertungsverbote, Seite)

Strate, Gerhard / Ventzke, Klaus-Ulrich: Unbeachtlichkeit einer Verletzung des § 137 Abs. 1 S. 1 StPO im Ermittlungsverfahren?, Strafverteidiger 1986, S. 30–34, (zit.: *Strate/Ventzke*, StV 1986, Seite)

Sujecki, Bartosz: Internationales Privatrecht und Cloud Computing aus europäischer Perspektive, Kommunikation & Recht 2012, S. 312–317, (zit.: *Sujecki*, K&R 2012, Seite)

Süptitz, Thomas / Utz, Christine / Eymann, Torsten: State-of-the-Art: Ermittlungen in der Cloud, Datenschutz und Datensicherheit 2013, S. 307–312, (zit.: *Süptitz/Utz/Eymann*, DuD 2013, Seite)

Sydow, Fritz:Kritik der Lehre von den „Beweisverboten", Würzburg 1976, (zit.: *Sydow*, Kritik der Lehre von den „Beweisverboten", Seite)

Szebrowski, Nickel: E-Mail-Beschlagnahme – Klärung durch den BGH, Multimedia und Recht 2009, S. V-VI, (zit.: *Szebrowski*, MMR 2009, Seite)

Szesny, André: Durchsicht von Daten gem. § 110 StPO, Journal der Wirtschaftsstrafrechtlichen Vereinigung e.V 2012, S. 228–235, (zit.: *Szesny*, WiJ 2012, Seite)

Taeger, Jürgen / Gabel, Detlev (Hrsg.): Kommentar zum BDSG, 2. Auflage, Frankfurt 2013, (zit.: *Bearbeiter* in: Taeger/Gabel-BDSG, §, Rn.)

Taeger, Jürgen / Pohle, Jan: Computerrechtshandbuch, 36. Ergänzungslieferung, Stand: Februar 2021, München 2021, (zit.: *Bearbeiter* in: Taeger/Pohle, ComputerR-HdB, Kap, Rn. 4)

Theile, Hans: Wahrheit, Konsens und § 257c StPO, Neue Zeitschrift für Strafrecht 2012, S. 666–671, (zit.: *Theile*, NStZ 2012, Seite)

Traub, Michael: Die Verwertbarkeit von Selbstgesprächen im Strafverfahren, Würzburg 2015, (zit.: *Traub*, Verwertbarkeit von Selbstgesprächen, Seite)

Trüg, Gerson / Habetha, Jörg: Beweisverwertung trotz rechtswidriger Beweisgewinnung – insbesondere mit Blick auf die „Liechtensteiner Steueraffäre", Neue Zeitschrift für Strafrecht 2008, S. 481–492, (zit.: *Trüg/Habetha*, NStZ 2008, Seite)

Trüg, Gerson / Habetha, Jörg: Die „Liechtensteiner Steueraffäre" – Strafverfolgung durch Begehung von Straftaten?, Neue Juristische Wochenschrift 2008, S. 887–890, (zit.: *Trüg/Habetha*, NJW 2008, Seite)

Trüg, Gerson / Kerner, Hans-Jürgen: Formalisierung der Wahrheitsfindung im (reformiert-) inquisitorischen Strafverfahren? Betrachtungen unter rechtsvergleichender Perspektiv, Festschrift für Reinhard Böttcher zum 70. Geburtstag, S. 191–212, Berlin 2007, (zit.: FS-Böttcher/*Trüg/Kerner*, Seite)

Trüg, Gerson: Einziehung bei Marktmanipulation und Zugriff auf E-Mails beim Provider, zgl. Besprechung von BGH, Beschluss v. 14.10.2020 – 5 StR 229/19, Juristenzeitung 2021, S. 560-565, (zit.: *Trüg*, JZ 2021, Seite)

Trüg, Gerson: Anmerkung zu BGH-Beschluss v. 22.09.2015 – 4 StR 355/15 – Beweisantrag auf Verlesung eines E-Mail-Ausdruckes als präsentes Beweismittel, Strafverteidiger 2016, S. 343–345, (zit.: *Trüg*, StV 2016, Seite)

Trüg, Gerson: Erkenntnisse aus der Untersuchung des US-amerikanischen plea bargaining-Systems für den deutschen Absprachendiskurs, Zeitschrift für die gesamte Strafrechtswissenschaft 2008, S. 331–374, (zit.: *Trüg*, ZStW 2008, Seite)

Trüg, Gerson: Quo curris, Strafverfahren? – Zum Verhältnis der objektiven Dimension der Beschleunigungsmaxime zur Wahrheitsfindung, Strafverteidiger 2010, S. 528–538, (zit.: *Trüg*, StV 2010, Seite)

Trüg, Gerson:Lösungskonvergenzen trotz Systemdivergenzen im deutschen und US-amerikanischen Strafverfahren, Tübingen 2003, (zit.: *Trüg*, Lösungskonvergenzen trotz Systemdivergenzen, Seite)

Valerius, Brian: Ermittlungsmaßnahmen im Internet, Juristische Rundschau 2007, S. 275–280, (zit.: *Valerius*, JR 2007, Seite)

Valerius, Brian: Grenzen des Großen Lauschangriffs – Verwertbarkeit eines aufgezeichneten Selbstgesprächs des Beschuldigten, Juristische Arbeitsblätter 2006, S. 15–17, (zit.: *Valerius*, JA 2006, Seite)

Ventzke, Klaus Ulrich: Die Widerspruchslösung des Bundesgerichtshofs – viel Getue um nichts?, Strafverteidiger 1997, S. 543–549, (zit.: *Ventzke*, StV 1997, Seite)

Ventzke, Klaus-Ulrich / Roxin, Claus: Verwertung einer einem Beweisverwertungsverbot unterliegenden Aussage mit Zustimmung des Betroffenen, zugleich Anm. zu BGH, Beschluss vom 05.08.2008 – 3 StR 45/08, Strafverteidiger 2009, S. 113–115, (zit.: *Ventzke/Roxin*, StV 2009, Seite)

Voigt, Paul: Weltweiter Datenzugriff durch US-Behörden – Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten, Multimedia und Recht 2014, S. 158–161, (zit.: *Voigt*, MMR 2014, Seite)

Volk, Klaus / Engländer, Armin: Grundkurs StPO, 9. Auflage, München 2018, (zit.: *Volk/Engländer*, GK StPO, §, Rn.)

Von der Lippe, Sabine: Die Widerspruchslösung der Rechtsprechung für strafprozessuale Beweisverwertungsverbote, Hamburg 2001, (zit.: *von der Lippe*, Die Widerspruchslösung der Rechtsprechung, Seite)

von Heintschel-Heinegg, Bernd: Selbstgespräche sind kein Beweis, Juristische Arbeitsblätter 2012, S. 395–396, (zit.: *von Heintschel-Heinegg*, JA 2012, Seite)

Voßkuhle, Andreas: Theorie und Praxis der verfassungskonformen Auslegung von Gesetzen durch Fachgerichte, Archiv für öffentliches Recht 2000, S. 177–201, (zit.: *Voßkuhle*, AöR 2000, Seite)

Wabnitz, Heniz-Bernd / Janovsky, Thomas (Hrsg.): Handbuch des Wirtschafts- und Steuerstrafrechts, 5. Auflage, München 2020, (zit.: *Bearbeiter* in: Handbuch des Wirtschafts- und Steuerstrafrechts, Kapitel, Rn.)

Walter, Tonio: Fair trial statt Nemo tenetur, Europäisierung des Rechts, S. 291–308, (zit.: *Walter* in: Europäisierung des Rechts, Seite)

Warg, Gunter:Anmerkungen zum Kernbereich privater Lebensgestaltung – Zugleich Besprechung von BGH, Urteil vom 22. 12. 2011, Neue Zeitschrift für Strafrecht 2012, S. 237–242, (zit.: *Warg*, NStZ 2012, Seite)

Warken, Claudia: Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus – Teil 1, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 2017, S. 289–298, (zit.: *Warken*, NZWiSt 2017, Seite)

Warken, Claudia: Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus – Teil 2, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 2017, S. 329–338, (zit.: *Warken*, NZWiSt 2017, Seite)

Warntjen, Maximilian: Der Kernbereich privater Lebensgestaltung und die Telekommunikationsüberwachung gemäß § 100a StPO, Kritische Justiz 2005, S. 276–286, (zit.: *Warntjen*, KJ 2005, Seite)

Warntjen, Maximilian: Heimliche Zwangsmaßnahmen und der Kernbereich, Baden-Baden 2007, (zit.: *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich, Seite)

Wassermann, Rudolf (Hrsg.): Alternativkommentare – Kommentar zur Strafprozessordnung, 1. Auflage, Band 2, §§ 94–212b, Berlin 1992, (zit.: *Bearbeiter* in: AK-StPO, §, Rn.)

Weber, Christoph / Meckbach, Anne: Äußerungsdelikte in Internetforen – zugleich Anmerkung zu LG Mannheim, Beschluss vom 13. 5. 2005 – 5 Qs 23/05, Neue Zeitschrift für Strafrecht 2006, S. 492–495, (zit.: *Weber/Meckbach*, NStZ 2006, Seite)

Weber, Michelle: Strafrecht und Sprachassistenz: „Alexa, verrätst du mich?" – „Das weiß ich leider nicht!", juris – Die Monatszeitschrift 2021, S. 252–256, (zit.: *Weber*, jM 2021, Seite)

Weichert, Thilo: Cloud Computing und Datenschutz, Datenschutz und Datensicherheit 2010, S. 679–687, (zit.: *Weichert*, DuD 2010, Seite)

Weißer, Bettina: Zeugnisverweigerungsrechte und Menschenwürde als Schutzschild gegenheimliche strafprozessuale Zugriffe auf Kommunikationsinhalte, Goltdammers Archiv 2006, S. 148–167, (zit.: *Weißer*, GA 2006, Seite)

Wenskat, Wolfgang: Der richterliche Augenschein im deutschen Strafprozess, Frankfurt 1988, (zit.: *Wenskat*, Der richterliche Augenschein, Seite)

Wenzel, Henning: Rechtliche Grundlagen der IT-Forensik, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 2016, S. 85 – 93, (zit.: *Wenzel*, NZWiSt 2016, Seite)

Wesemann, Horst / Müller, Anissa:Das gem. $ 136a Abs. 3 StPO unverwertbare Geständnis und seine Bedeutung im Rahmen der Strafzumessung, Strafverteidiger Forum 1998, S. 113–116, (zit.: *Wesemann/Müller*, StraFo 1998, Seite)

Wessels, Johannes / Hettinger, Michael / Engländer, Armin: Strafrecht – Besonderer Teil 1, 44. Auflage, Heidelberg 2020, (zit.: *Wessels/Hettinger/Engländer*, Strafrecht BT I, Rn.)

Weßlau, Edda: Gefährdungen des Datenschutzes durch den Einsatz neuer Medien im Strafprozess, Zeitschrift für die gesamte Strafrechtswissenschaft 2001, S. 681–708, (zit.: *Weßlau*, ZStW 2001, Seite)

Weßlau, Edda: Gespaltene Tatsachenfeststellungen, Überkreuzverwertungen und advokatorische Dilemmata – Beweisverwertung zum Nachteil von Mitbeschuldigten, Strafverteidiger 2010, S. 41–45, (zit.: *Weßlau*, StV 2010, Seite)

Wicker, Magda: Cloud Computing und staatlicher Strafanspruch: Strafrechtliche Risiken und strafprozessuale Ermittlungsmöglichkeiten in der Cloud, Baden-Baden 2016, (zit.: *Wicker*, Cloud Computing und staatlicher Strafanspruch, Seite)

Wicker, Magda: Die Neuregelung des § 100j StPO auch beim Cloud Computing Zugriff auf Zugangsdaten zur Cloud nach der neuen Bestandsdatenauskunft, Multimedia und Recht 2014, S. 298–302, (zit.: *Wicker*, MMR 2014, Seite)

Wicker, Magda: Durchsuchung in der Cloud – Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, Multimedia und Recht 2013, S. 765–769, (zit.: *Wicker*, MMR 2013, Seite)

Wicker, Magda: Ermittlungsmöglichkeiten in der Cloud, DSRI-Tagungsband 2013, S. 981–1001, (zit.: *Wicker*, DSRITB 2013, Seite)

Widmaier, Gunter: Mitwirkungspflicht des Verteidigers in der Hauptverhandlung und Rügeverlust(?), Neue Zeitschrift für Strafrecht 1992, S. 519–523, (zit.: *Widmaier*, NStZ 1992, Seite)

Wiegand, Dorothee: Hier spricht dein Computer, Magazin für Computertechnik 2020, Heft 14, S. 118–121, (zit.: *Wiegand*, c´t 2020, Heft, Seite)

Wiemers, Matthias: Teilweise Verfassungswidrigkeit des BKA-Gesetzes, Neue Zeitschrift für Verwaltungsrecht 2016, S. 839–841, (zit.: *Wiemers*, NVwZ 2016, Seite)

Willer, Christoph / Hoppen, Peter:Computerforensik – Technische Möglichkeiten und Grenzen, Computer und Recht 2007, S. 610–616, (zit.: *Willer/Hoppen*, CR 2007, Seite)

Winkemann, Jule: Informationspflichten im Voice-Commerce, Computer und Recht 2020, S. 451–457, (zit.: *Winkemann*, CR 2020, Seite)

Wohlers, Wolfgang: Anm. zu BGH Urteil vom 22. 12. 2011 – 2 StR 509/10, Juristische Rundschau 2012, S. 389–391, (zit.: *Wohlers*, JR 2012, Seite)

Wohlers, Wolfgang: Die Hypothese rechtmäßiger Beweiserlangung – ein Instrument zur Relativierung unselbständiger Verwertungsverbote?, Festschrift für Gerhard Fezer zum 70. Geburtstag, S. 61–86, Berlin 2008, (zit.: FS-Fezer/*Bearbeiter*, Seite)

Wohlers, Wolfgang: Die Nichtbeachtung des Richtervorbehalts, Strafverteidiger 2008, S. 434–442, (zit.: *Wohlers*, StV 2008, Seite)

Wohlers, Wolfgang: Zur (Un-)Verwertbarkeit strafrechtswidrig erhobener Bild- und Audioaufzeichnungen des Tatgeschehens, Juristische Rundschau 2016, S. 509–514, (zit.: *Wohlers*, JR 2016, Seite)

Wölfl, Bernd:Die Verwertbarkeit heimlicher privater Ton- und Bildaufnahmen im Strafverfahren, Frankfurt 1997, (*Wölfl*, Verwertbarkeit heimlicher privater Ton- und Bildaufnahmen, Seite)

Wollweber, Harald: Anm. zu BGH Beschluss vom 15. August 2000 – 5 StR 223/00, Zeitschrift für Wirtschafts- und Steuerstrafrecht 2001, S. 182–183, (zit.: *Wollweber*, wistra 2001, Seite)

Wölm, Benjamin: Schutz der Internetkommunikation und „heimliche Internetaufklärung", Hamburg 2014, (zit.: *Wölm*, Schutz der Internetkommunikation und heimliche Internetaufklärung, Seite)

Wolter, Jürgen (Hrsg): Systematischer Kommentar zum Strafgesetzbuch, 9. Auflage, Band IV, §§ 174–241a StGB, Köln 2017, (zit.: *Bearbeiter* in: SK-StGB, §, Rn.)

Wolter, Jürgen (Hrsg): Systematischer Kommentar zur Strafprozessordnung, 5. Auflage, Band II, §§ 94–136a, Köln 2016, (zit.: *Bearbeiter* in: SK-StPO, §, Rn.)

Wolter, Jürgen: Fernwirkung von Beweisverwertungsverboten, Neue Zeitschrift für Strafrecht 1984, S. 276–278, (zit.: *Wolter*, NStZ 1984, Seite)

Wolter, Jürgen: Kriminalpolitik und Strafprozessrechtssystem, Festschrift für Claus Roxin zum 70. Geburtstag, S. 1141–1171, Berlin 2001, (zit.: FS-Roxin 2001/*Wolter*, Seite)

Wolter, Jürgen: Menschenwürde, Kernbereich privater Lebensgestaltung und Recht auf Leben, Festschrift für Wilfried Küper zum 70. Geburtstag, S. 707–722, Heidelberg 2007, (zit.: FS-Küper/*Wolter*, Seite)

Wolter, Jürgen: Repressive und präventive Verwertung tagebuchartiger Aufzeichnungen, Strafverteidiger 1990, S. 175–184, (zit.: *Wolter*, StV 1990, Seite)

Wolter, Jürgen: Wider das systemlose Abwägungs-Strafprozessrecht, Festschrift für Claus Roxin zum 80. Geburtstag, S. 1245–1268, Berlin 2011, (FS-Roxin/*Wolter*, Seite)

Wormer, Elke: Der strafrechtliche Schutz der Privatsphäre vor Missbräuchen mit Tonaufnahme und Abhörgeräten – Eine Abhandlung zu § 201 StGB, Mannheim 1977, (zit.: *Wormer*, Der strafrechtliche Schutz der Privatsphäre, Seite)

Würtenberger, Thomas / Heckmann, Dirk / Tanneberger, Steffen:Polizeirecht in Baden-Württemberg, 7. Auflage, Heidelberg 2017, (zit.: *Würtenberger/Heckmann/Tanneberger*, Polizeirecht, §, Rn.)

Zabel, Benno:Kernbereichsschutz und Verwertungsdogmatik, Anm. zu BGH, Urt. v. 22.12.2011 – 2 StR 509/10, Zeitschrift für das Juristische Studium 2012, S. 563–567, (zit.: *Zabel*, ZJS 2012, Seite)

Zeitler, Stefan / Trurnit, Christoph: Polizeirecht für Baden-Württemberg, 3. Auflage, Stuttgart 2014, (zit.: *Zeitler/Turnit*, Polizeirecht, Rn.)

Zerbes, Ingeborg / El-Ghazi, Mohamad: Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, Neue Zeitschrift für Strafrecht 2015, S. 425–433, (zit.: *Zerbes/El-Ghazi*, NStZ 2015, Seite)

Zeyher, Lukas: Strafprozessuale Beweisverwertung von privatem Videomaterial am aktuellen Beispiel der Dashcam, Berlin 2021, (zit.: *Zeyher*, Strafprozessuale Beweisverwertung von privatem Videomaterial, Seite)

Zimmermann, Till: Das Selbstgespräch und der Kernbereich privater Lebensgestaltung, Goltdammers Archiv 2013, S. 162–173, (zit.: *Zimmermann*, GA 2013, Seite)

Zimmermann, Till: Der strafprozessuale Zugriff auf E-Mails, Juristische Arbeitsblätter 2014, S. 321–327, (zit.: *Zimmermann*, JA 2014, Seite)

Zöller, Mark: Heimliche und verdeckte Ermittlungsmaßnahmen im Strafverfahren, Zeitschrift für die gesamte Strafrechtswissenschaft 2012, S. 411–439, (zit.: *Zöller*, ZStW 2012, Seite)

Zöller, Mark:Heimlichkeit als System, Strafverteidiger Forum 2008, S. 15–25, (zit.: *Zöller*, StraFo 2008, Seite)

Zwiehoff, Gabriele: Der große Lauschangriff, Baden-Baden 2000, (zit.: *Bearbeiter* in: Zwiehoff, Der große Lauschangriff, Seite)