

Schriften zum Strafrechtsvergleich

Band 17

**Datenerhebungen
im Ermittlungsverfahren und
rechtsstaatliche Beschränkungen**

Rechtsvergleich zwischen Deutschland und Südkorea

Von

Joongwook Park



Duncker & Humblot · Berlin

JOONGWOOK PARK

Datenerhebungen im Ermittlungsverfahren
und rechtsstaatliche Beschränkungen

Schriften zum Strafrechtsvergleich

Herausgegeben von

Prof. Dr. Dr. Eric Hilgendorf, Würzburg und
Prof. Dr. Brian Valerius, Bayreuth

Band 17

Datenerhebungen im Ermittlungsverfahren und rechtsstaatliche Beschränkungen

Rechtsvergleich zwischen Deutschland und Südkorea

Von

Joongwook Park



Duncker & Humblot · Berlin

Die Juristische Fakultät der Ludwig-Maximilians-Universität München
hat diese Arbeit im Jahre 2021 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

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

Alle Rechte vorbehalten
© 2023 Duncker & Humblot GmbH, Berlin
Satz: 3w+p GmbH, Rimpf
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 2364-8155
ISBN 978-3-428-18696-9 (Print)
ISBN 978-3-428-58696-7 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☼

Internet: <http://www.duncker-humblot.de>

Vorwort

Die vorliegende Arbeit, die von mir Ende Februar 2021 zur Promotionsprüfung an der Juristischen Fakultät der Ludwig-Maximilians-Universität München abgegeben wurde, wurde im April 2022 als Dissertation angenommen.

Die in dieser Arbeit behandelte Datenerhebung im Strafverfahren ist eines der am meisten diskutierten Themen im weltweiten Digitalisierungsprozess und umfasst zahlreiche Einzelfragen. In den letzten 20 Jahren wurden in Deutschland und Südkorea einschlägige Gesetze und Vorschriften zur Datenerhebung erlassen und langanhaltende Diskussionen führten zur stetigen Veränderung der Gesetzeslage. Ein Ende des Anpassungsprozesses ist derzeit nicht in Sicht. Diese Arbeit wurde zum Zeitpunkt der Abgabe Anfang 2021 verfasst. In Deutschland wurden seitdem jedoch einerseits durch die beiden Änderungsgesetze vom 30.3.2021 (BGBl. I S. 441 & 448) § 100k StPO zur Erhebung von Nutzungsdaten bei Telemediendiensten geschaffen und §§ 100g, 100j, 101a und 101b StPO geändert, sowie andererseits durch das Gesetz zur Fortentwicklung der StPO vom 25.6.2021 (BGBl. I S. 2099) § 95a StPO zur Zurückstellung der Benachrichtigung und zum Offenbarungsverbot und § 163g StPO zur automatischen Kennzeichenerfassung geschaffen und §§ 99f, 101, 104 und 110 StPO überarbeitet. Dies konnte in der vorliegenden Arbeit nicht berücksichtigt werden.

Die Fertigstellung dieser Arbeit war eine große Herausforderung für mich und eine schwierige und langwierige Aufgabe. Insbesondere die seit Anfang 2020 andauernde Pandemie hat die Fertigung meiner Arbeit erheblich behindert.

Es gibt so viele, denen ich danken sollte, aber zunächst möchte ich meinen besonderen Dank an meinen Betreuer, Herrn Prof. h.c. Dr. *Schünemann*, aussprechen, der an mich geglaubt und geduldig auf meine Ergebnisse gewartet hat. Nicht vergessen möchte ich den leider verstorbenen Herrn Prof. Dr. *Vogel*, der mir zum ersten Mal die Möglichkeit gab, in Deutschland zu studieren. Ich wünsche ihm ewige Ruhe in Frieden. Mein Dank gilt weiterhin Herrn Prof. Dr. *Zöller*, der als zweiter Gutachter meine Arbeit gelesen und hilfreiche Kommentare abgegeben hat.

Mein besonderer Dank gilt auch den koreanischen Beratern, Herrn Prof. Dr. *Kuk Cho*, Herrn Prof. Dr. *Huigi Sim* und Herrn Prof. Dr. *Changkook Kwon*, die mich während meines Studiums in Deutschland mit vielen akademischen Ratschlägen unterstützt haben. Zugleich möchte ich meinen Kollegen und Freunden, Herrn Dr. *Sunki Hong*, Herrn Dr. *Hee-Young Park*, Herrn Prof. Dr. *Sung-Eun Park*, Herrn Dr. *Jinhwan Chang*, Frau Dr. *Hyunjung Lee* und Herrn Dr. *Seung-Uk Yang*, die zur selben Zeit in Deutschland studiert haben, herzlich danken.

Weiter möchte ich herzlich danken der Familie *Kyle Namkoong*, der Familie *Hyung-taek Lim*, der Familie *Jung-soo Kim*, der Familie *Eunho Lee* und der Familie *Se-won Lee*, auch der Familie *Seongyeon Kim*.

Schließlich ist die Fertigstellung dieser Arbeit im Wesentlichen der Unterstützung und Geduld meiner Eltern und meiner Familie zu verdanken. Zunächst einmal haben meine Eltern, *Hyung-Woo Park* und *Keumok Jin*, immer versucht, mir auch aus der Ferne Ruhe zu geben. Ich möchte mich weiterhin ganz herzlich bei meiner lieben Familie bedanken. Meine Frau, *Sookyung Ham*, war während der Promotion immer an meiner Seite und die beiden dazwischen geborenen Töchter, *Jueun* und *Seo-eun*, ließen mich die Schwierigkeiten des Studiums vergessen. Sie sind der größte Schatz, den ich in Deutschland erworben habe.

Seoul, im Juli 2022

Joongwook Park

Inhaltsverzeichnis

Kapitel 1

| | |
|--|----|
| Vorbemerkung | 21 |
| A. Ausgangspunkte | 21 |
| I. Aktuelle Lage | 21 |
| II. Historische Übersicht | 23 |
| 1. Entstehung und Entwicklung betreffender Vorschriften in Deutschland | 23 |
| 2. Entstehung und Entwicklung betreffender Vorschriften in Südkorea | 28 |
| B. Forschungsziel und Gang der Untersuchung | 35 |

Kapitel 2

Fortschritt der Informationstechnik, Rechtsstaatsprinzip und maßgebliche Grundrechte

| | |
|---|----|
| Fortschritt der Informationstechnik, Rechtsstaatsprinzip und maßgebliche Grundrechte | 37 |
| A. Fortschritt der Informationstechnik und Rechtsstaatsprinzip | 37 |
| I. Änderung der Realität und neue Gefährdungen | 37 |
| 1. Informationstechnik und ihre Bedeutung für die Persönlichkeitsentfaltung | 37 |
| 2. Ansammlung und Konzentration von Daten und neuartige Gefährdungen | 39 |
| a) Ansammlung und Konzentration von Daten – Eigenschaften elektronischer Daten und Arten der Telekommunikationsdaten | 39 |
| b) Neuartige Gefährdungen | 42 |
| II. Aufgaben des Staates und rechtsstaatliche Grenzen | 44 |
| 1. Aufgaben des Staates und Anpassung an die Veränderung der Realität | 44 |
| 2. Strafverfahrensrecht im Rechtsstaat | 46 |
| a) Rechtsstaatsprinzip und Grenzen der Ermittlungshandlungen | 46 |
| b) Fair-Trial-Grundsatz und Justizförmigkeit des Strafverfahrens | 48 |
| III. Normenbestimmtheit und -klarheit sowie Verhältnismäßigkeit | 51 |
| 1. Gebot der Normenbestimmtheit und -klarheit | 51 |
| a) Bedeutung | 51 |
| b) Zweckbindung und Verbot der Zweckänderung bzw. -entfremdung | 53 |
| 2. Grundsatz der Verhältnismäßigkeit | 54 |
| a) Bedeutung und Prüfungsstruktur | 54 |
| b) Verhältnismäßigkeit im engeren Sinne: Gesamtabwägung | 56 |

| | |
|---|----|
| c) Datenzugriff und Abwägung | 58 |
| aa) Informationstechnische Gegebenheiten – mitsamt einer Veränderung der Wahrnehmung der Realität des <i>BVerfG</i> | 59 |
| bb) Heimlichkeit der Maßnahmen und umfassende Datenerhebung | 61 |
| IV. Zusammenfassung und Zwischenfazit | 62 |
| B. Maßgebliche Grundrechte | 63 |
| I. Vorrede | 63 |
| II. Allgemeines Persönlichkeitsrecht und Schutz des Kernbereichs privater Lebens- gestaltung | 64 |
| 1. Allgemeines Persönlichkeitsrecht: Schutz des privaten Lebensbereichs | 64 |
| a) Rechtsgrundlage und Bedeutung | 64 |
| b) Verfassungsrechtliches Beweisverbot | 67 |
| 2. Schutz des Kernbereichs privater Lebensgestaltung | 68 |
| a) Rechtsgrundlage und Bedeutung | 68 |
| b) Schwierigkeit des Schutzes in der Informationsgesellschaft | 70 |
| c) § 100d StPO | 71 |
| 3. Zusammenfassung | 72 |
| III. Recht auf informationelle Selbstbestimmung und Computer-Grundrecht | 73 |
| 1. Recht auf informationelle Selbstbestimmung: Volkszählungsurteil | 73 |
| a) Erkenntnis- bzw. Erwägungsgründe und Schutzbereich | 73 |
| b) Eingriffsschwellen | 75 |
| 2. Computer-Grundrecht: Urteil zur Online-Durchsuchung | 75 |
| a) Erkenntnis- bzw. Erwägungsgründe und Schutzbereich | 75 |
| b) Eingriffsschwellen | 77 |
| 3. Verfassungsrechtliche Kriterien zum Datenschutz | 77 |
| IV. Der Schutz des Fernmeldegeheimnisses: Art. 10 GG | 79 |
| 1. Spezifischer Schutzbedarf | 79 |
| 2. Schutzbereich | 80 |
| 3. Verhältnis zum allgemeinen Persönlichkeitsrecht | 82 |
| V. Unverletzlichkeit der Wohnung: Art. 13 GG | 83 |
| 1. Schutzbereich und Eingriffsart | 83 |
| 2. Verhältnis zu sonstigen Grundrechten | 84 |
| 3. Beschränkungen | 85 |
| VI. Zusammenfassung und Zwischenfazit | 86 |
| C. Verfassungsrechtlicher Datenschutz und strafverfahrensrechtliches Prinzip des Aus- schlusses von illegal erlangten Beweisen in Südkorea | 87 |
| I. Vorrede | 87 |

- II. Verfassungsrechtlicher Datenschutz 88
 - 1. Recht auf informationelle Selbstbestimmung: Fingerabdruckspeicherungsbe-
schluss 88
 - a) Hintergrund und verfassungsrechtliche Grundlage 88
 - b) Schutzbereich 91
 - c) Beschränkung 92
 - 2. Schutz des Kommunikationsgeheimnisses: Art. 18 K-Verf 93
 - 3. Zusammenfassung und Zwischenfazit 94
- III. Prinzip des Ausschlusses von illegal erlangten Beweisen: § 308a K-StPO 95
 - 1. Allgemeines 95
 - 2. Die Verankerung des Ausschlussprinzips und deren Sinn 96
 - a) Kontroverse vor der Verankerung: Grundlage des Ausschlussprinzips 96
 - b) Der Sinn der Verankerung 99
 - 3. Das Ausschlussprinzip bei Beweismitteln nicht in Worten: Anwendungskrite-
rien des § 308a K-StPO 100
 - a) Fragestellung 100
 - b) *K-OGHE* (Plenum) vom 15. 11. 2007–2007 Do 3061: „Grundsätzlicher
Ausschluss, ausnahmsweise Zulässigkeit“ 101
 - 4. Zusammenfassung und Zwischenfazit 102

Kapitel 3

Heimliche Zwangsmaßnahmen 104

- A. Heimliche Ermittlungen und Zwangsmaßnahmen 104
 - I. Zulässigkeit heimlicher Ermittlungen und kriminalistische Zwangsmaßnahmen 104
 - 1. Zulässigkeit heimlicher Ermittlungen 104
 - 2. Kriminalistische Zwangsmaßnahmen 105
 - 3. Heimliche Zwangsmaßnahmen 106
 - a) Ausnahmsweiser und eigenständiger Charakter 106
 - b) Verfassungsrechtliche Rechtfertigung – Ausschluss von Rundumüberwa-
chung 108
 - II. „Heimlichkeit“ bei heimlichen Zwangsmaßnahmen 109
 - 1. Durchführung „ohne Wissen des Betroffenen“ 109
 - 2. Verhältnis zum Recht auf rechtliches Gehör 112
 - 3. Verhältnis zur Bekanntmachung und Benachrichtigung 113
 - 4. Exkurs: Heimlichkeit in der Verkehrsdatenerhebung (§§ 100g, 101a StPO) ... 116
 - III. Zulässigkeitsvoraussetzungen zu den heimlichen Zwangsmaßnahmen – i. R. d.
Erhebung und Verwendung personenbezogener Daten 118
 - 1. Vorrede 118
 - 2. Qualifizierte Eingriffsvoraussetzungen 119

| | |
|--|-----|
| 3. Strenge verfahrensrechtliche Sicherungen | 121 |
| a) Anforderungen an Transparenz | 121 |
| b) Richtervorbehalt | 121 |
| c) Effektiver Rechtsschutz | 123 |
| d) Administrative aufsichtliche Kontrolle | 126 |
| e) Berichtspflichten gegenüber Parlament | 126 |
| f) Löschungs- und Protokollierungspflicht | 126 |
| IV. Zwischenfazit – Bedarf an qualifizierter Kontrolle gegen heimliche Zwangsmaßnahmen | 127 |
| B. Ermächtigungsgrundlagen für „zwangsmäßige bzw. heimliche Ermittlungsmaßnahmen“ im 8. Abschnitt des Ersten Buches der StPO | 127 |
| I. Allgemeines | 127 |
| 1. Konstruktion der Ermächtigungsgrundlagen zur Beweissicherung in der StPO | 127 |
| 2. Die allgemeinen Vorschriften der Beschlagnahme und Durchsuchung: §§ 94 ff., 102 ff. StPO | 129 |
| II. Eigene Ermächtigungen: §§ 99 bis 101b, 110a und 163f StPO | 130 |
| 1. Überblick | 130 |
| 2. Wohnraumüberwachung und Online-Durchsuchung | 132 |
| a) Wohnraumüberwachung | 133 |
| b) Online-Durchsuchung | 135 |
| c) Kritik an der Gesetzgebung zur Online-Durchsuchung (und Quellen-TKÜ) | 136 |
| 3. TKÜ und Postbeschlagnahme | 141 |
| a) TKÜ | 141 |
| b) Quellen-TKÜ | 143 |
| c) Postbeschlagnahme | 146 |
| 4. Erhebung von Verkehrs- und Standortdaten | 147 |
| 5. Auskunft über Bestandsdaten und Zugangssicherungs-codes | 151 |
| a) Bestandsdatenauskunft | 151 |
| b) Beschaffung der Zugangssicherungs-codes | 152 |
| 6. Sonstige verdeckte Maßnahmen | 156 |
| a) Akustische Überwachung außerhalb von Wohnraum | 156 |
| b) Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten | 157 |
| c) Verdeckter Ermittler und längerfristige Observation | 159 |
| d) Herstellung von Bildaufnahmen und Einsatz sonstiger technischer Mittel | 160 |
| III. Zusammenfassung und Zwischenfazit | 162 |
| C. Ermächtigungsgrundlagen für heimlichen Zugriff auf die auf dem Server des Dienst-anbieters gespeicherten Daten | 163 |
| I. Fragestellung | 163 |
| II. Technische Vorgänge nach Kommunikationsart sowie einschlägige Grundrechte | 164 |
| 1. E-Mail-Verkehr | 165 |

| | |
|---|-----|
| 2. Nachrichten in sozialen Netzwerken und Internet-Foren | 166 |
| 3. Cloud-Computing | 168 |
| III. Ermächtigungsgrundlagen | 170 |
| 1. Zugriff auf beim E-Mail- und Soziales-Netzwerk-Server gespeicherte Nachrichteninhalte | 170 |
| a) Anwendbarkeit von § 99 StPO | 170 |
| b) Anwendbarkeit von § 100a StPO und Anforderung an eine Neuregelung .. | 172 |
| c) Sonstige verdeckte Ermittlungsmaßnahmen bei geschlossenen sozialen Netzwerken und Internet-Foren | 176 |
| 2. Zugriff auf beim Cloud-Speicher gespeicherte Daten | 177 |
| IV. Zusammenfassung und Zwischenergebnisse | 180 |
| D. Ermächtigungsgrundlagen für heimliche Ermittlungsmaßnahmen in Südkorea | 180 |
| I. Vorrede – Hintergrundwissen zum Verständnis der Diskussionen in Südkorea .. | 180 |
| 1. Übersicht | 180 |
| 2. Eigene Merkmale von K-KGSG | 183 |
| II. Heimliche Ermittlungsmaßnahmen zur Beweissicherung und ihre Ermächtigung | 187 |
| 1. TKÜ und Postzensur | 187 |
| a) Eingriffsvoraussetzungen und präventive Verfahrenskontrolle | 188 |
| aa) Eingriffsvoraussetzungen: § 5 K-KGSG | 188 |
| bb) präventive Verfahrenskontrolle: § 6 K-KGSG | 191 |
| b) TKÜ im Eilfall: § 8 K-KGSG | 192 |
| c) Durchführung sowie Schweigepflichten und Einschränkung der Verwertung: §§ 9, 11, 12, 15 K-KGSG | 193 |
| d) Benachrichtigung und effektiver Rechtsschutz: §§ 9a, 9b und 13b K-KGSG | 195 |
| aa) Übersicht über die Inhalte der Vorschriften | 195 |
| bb) Probleme und Kritik | 197 |
| cc) Mangel an Verfahren zum nachträglichen Rechtsschutz | 200 |
| e) Paket-Überwachung | 201 |
| 2. Erhebung von Verkehrs- und Standortdaten | 205 |
| a) Eingriffsvoraussetzungen und präventive Verfahrenskontrolle: § 13 Abs. 1, 3, 4 und 9 K-KGSG | 205 |
| b) Nachträgliche Aufsicht und Benachrichtigung: § 13 Abs. 5–8 und § 13d sowie § 13b K-KGSG | 208 |
| c) Echtzeit-Lokalisierung und Funkzellenabfrage: § 13 Abs. 2 K-KGSG | 208 |
| aa) Erhebung der Standortdaten in Echtzeit durch Mobiltelefone | 209 |
| bb) Funkzellenabfrage | 211 |
| cc) Zusammenfassung und Zwischenfazit | 213 |
| 3. Bestandsdatenauskunft: § 83 K-TKGG (= § 54 K-TKGG a.F.) | 214 |
| 4. Das Abhören von nichtöffentlichen Gesprächen: § 14 K-KGSG | 219 |
| 5. Einsatz eines eigenständigen GPS-Trackers | 221 |

| | |
|--|-----|
| III. Zusammenfassung und Zwischenfazit | 221 |
|--|-----|

Kapitel 4

Anwendungsbereich und Verfahrensgarantien allgemeiner Vorschriften der Beschlagnahme und Durchsuchung 223

| | |
|--|-----|
| A. Vorrede | 223 |
| B. Abgrenzung nach dem Gebot der Normenbestimmtheit und -klarheit | 225 |
| I. Dürfen elektronische Daten Gegenstände der Beschlagnahme und Durchsuchung sein? – Beschlagnahmefähige Gegenstände | 225 |
| 1. Fragestellung und Meinungsstreit | 225 |
| 2. Zwischenfazit | 229 |
| II. Sind eine „heimliche“ Beschlagnahme und Durchsuchung aufgrund der §§ 94 ff., 102 ff. StPO zulässig? | 229 |
| 1. Fragestellung | 229 |
| 2. Meinungsstreit | 230 |
| a) Eine Mindermeinung: Zulässigkeit heimlicher Durchsuchung | 230 |
| b) Herrschende Meinung: Unzulässigkeit heimlicher Durchsuchung | 230 |
| aa) Einfacher Richtervorbehalt | 230 |
| bb) Das Durchführungsverfahren der Durchsuchung gemäß §§ 102 ff. StPO | 231 |
| cc) Rechtssystematischer Vergleich zu §§ 99 ff. StPO | 238 |
| 3. Zwischenfazit | 239 |
| III. Rechtfertigen §§ 94 ff., 102 ff. StPO eine offene Sicherstellung der „beim Server des ISP gespeicherten“ Daten? | 239 |
| 1. Vorrede | 239 |
| 2. Bestimmung der Ermächtigung | 240 |
| a) Herkömmliche schematische Einstellung und eine Wende des Denkens durch das <i>BVerfG</i> | 240 |
| b) Kritik an der Entscheidung des <i>BVerfG</i> | 242 |
| c) Gegenargumente | 243 |
| 3. Zwischenfazit | 245 |
| C. Verfahrensrechtliche Kontrolle nach dem Verhältnismäßigkeitsgrundsatz | 246 |
| I. Bilden die §§ 94 ff., 102 ff. StPO eine ausreichende gesetzliche Grundlage für die „offene, aber umfassende Sicherstellung“ der Daten? | 246 |
| 1. Fragestellung | 246 |
| 2. Stellungnahme des <i>BVerfG</i> | 247 |
| 3. Teilweise Kritik | 248 |
| 4. Exkurs: Erhebung der Zugangssicherungs-codes und Herausgabe unverschlüs- selter Daten in offenen Ermittlungen | 250 |
| a) Einleitung | 250 |

- b) Beauskunftung von Zugangssicherungs-codes und Anordnung von Ordnungs- und Zwangsmitteln 251
 - c) Herausgabe unverschlüsselter Daten 253
- II. Richtervorbehalt 255
 - 1. Grundsatz – richterliche Anordnung 255
 - a) Sinn und Zweck 255
 - b) Form 258
 - c) Richterlicher Beschluss 259
 - aa) Durchsuchungsobjekt 260
 - bb) Zu beschlagnahmende Gegenstände 261
 - cc) Verhältnismäßigkeit der Maßnahmen sowie Art und Weise ihrer Durchführung 263
 - dd) Durchsuchungsanordnung i. V.m. einer Beschlagnahmeanordnung ... 264
 - 2. Ausnahmsweise Ausschluss – nichtrichterliche Anordnung 267
 - a) Eilkompetenz 267
 - b) Voraussetzung – „Gefahr im Verzug“ 268
 - c) Eilzuständigkeit 271
 - d) Justiziabilität – Dokumentations- und Begründungspflichten 272
 - e) Gerichtliche nachträgliche Kontrolle: § 98 Abs. 2 StPO 273
 - 3. Exkurs – Aushöhlung des Richtervorbehalts in der Praxis 275
 - a) Kritik an der Praxis 275
 - b) Strukturelle und organisatorische Grenzen 277
 - c) Eine Alternative zur Lösung 278
- III. Durchsicht von Papieren: § 110 StPO 279
 - 1. Allgemeines 279
 - a) Sinn und Zweck des § 110 StPO 279
 - b) Charakter der „Durchsicht“ gemäß § 110 StPO 281
 - c) Bedarf an Verwendung, aber die Umgehung in der Praxis 282
 - 2. Tatbestände 284
 - a) Durchsicht von Papieren 284
 - aa) Papiere 284
 - bb) Durchsicht 284
 - cc) Erweiterung der Durchsicht um externe Speichermedien: Abs. 3 286
 - b) Befugnisse zur Durchsicht 292
 - aa) Zur Durchsicht befugte Beamte: Abs. 1 292
 - bb) Andere zur Durchsicht nicht befugte Beamte: Abs. 2 294
 - cc) Umgehung der Beschränkung der Durchsichtsbefugnis in der Praxis .. 295
 - 3. Vorläufige Sicherstellung 297
 - a) Begriff und Funktion 297
 - b) Die Fälle, in denen einer vorläufigen Sicherstellung Rechnung zu tragen ist 299

| | |
|--|-----|
| c) Begrenzung der Fortdauer der Durchsicht | 300 |
| d) Antrag auf gerichtliche Bestätigung bzw. Entscheidung | 302 |
| 4. Zufallsfunde: § 108 StPO | 303 |
| 5. Beendigung der Durchsicht | 307 |
| 6. Zusammenfassung und Zwischenfazit | 309 |
| IV. Verfahrensbalance i. R. d. Beschlagnahme und Durchsicherung von Papieren | 310 |
| 1. Vorrede | 310 |
| 2. Anwesenheitsrecht des Betroffenen und seines Verteidigers | 312 |
| a) Meinungsstreit und Stellungnahme des <i>BVerfG</i> | 312 |
| b) Begründung für das Anwesenheitsrecht | 313 |
| 3. Zwischenfazit | 315 |
| D. Anwendungsbereich und Verfahrenskontrolle der allgemeinen Vorschriften der Beschlagnahme und Durchsicherung in der K-StPO | 317 |
| I. Übersicht | 317 |
| II. Beschlagnahme und Durchsicherung im Ermittlungsverfahren: §§ 106 ff. i. V. m. §§ 215 ff. K-StPO | 319 |
| 1. Vorbemerkung | 319 |
| 2. Voraussetzungen und Gegenstände: §§ 106–112 und 215 K-StPO | 319 |
| 3. Verfahren | 322 |
| a) Antrag und Erlass der Anordnung in schriftlicher Form | 322 |
| b) Durchführung der Anordnung | 324 |
| c) Verfahren nach der Durchführung | 327 |
| d) Beschlagnahme und Durchsicherung ohne richterliche Anordnung: §§ 216–218, 220 K-StPO | 327 |
| e) Verwahrung und (Quasi-)Rückgabe der beschlagnahmten Gegenstände | 331 |
| f) Nachweis der Identität elektronischer Daten | 332 |
| 4. Beschwerde gegen die Art und Weise der Durchführung: § 417 K-StPO | 333 |
| III. Einzelne Streitpunkte | 334 |
| 1. Dürfen elektronische Daten Gegenstände der Beschlagnahme und Durchsicherung sein? | 334 |
| 2. Rechtfertigen die allgemeinen Vorschriften eine „heimliche“ Sicherstellung der „beim Server des ISP gespeicherten“ Daten? | 335 |
| 3. Ist Netzwerkdurchsicherung bzw. grenzüberschreitende Durchsicherung zulässig? | 337 |
| 4. Kopie und Mitnahme sämtlicher Daten, Teilnahmerecht und Zufallsfunde | 339 |
| a) Charakter der Kopie und Mitnahme sämtlicher Daten und Gewährleistung des Teilnahmerechts | 339 |
| b) Zufallsfunde | 342 |
| IV. Zusammenfassung und Zwischenfazit | 343 |

Inhaltsverzeichnis 15

Kapitel 5

Schlussbemerkung 347

Literaturverzeichnis 351

Stichwortverzeichnis 364

Abkürzungsverzeichnis

| | |
|----------|---|
| a. A. | andere/-r Ansicht/Auffassung |
| a. a. O. | am angegebenen Ort |
| Abs. | Absatz |
| abw. | abweichend |
| a. E. | am Ende |
| a. F. | alte Fassung |
| AG | Amtsgericht |
| Alt. | Alternative |
| Art. | Artikel |
| Aufl. | Auflage |
| BDSG | Bundesdatenschutzgesetz |
| BfV | Bundesamt für Verfassungsschutz |
| BGBI. I | Bundesgesetzblatt Teil I |
| BGH | Bundesgerichtshof |
| BGHSt | Entscheidungssammlung des BGH in Strafsachen |
| BGHZ | Entscheidungssammlung des BGH in Zivilsachen |
| BAK | Bundeskriminalamt |
| BKAG | Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) |
| BND | Bundesnachrichtendienst |
| BRD | Bundesrepublik Deutschland |
| BR-Drs. | Drucksache des Bundesrates |
| BT-Drs. | Drucksache des Bundestages |
| BVerfG | Bundesverfassungsgericht |
| BVerfGE | Entscheidungen des BVerfG |
| bzw. | beziehungsweise |
| CKÜ | Übereinkommen über Computerkriminalität (SEV Nr. 185), Budapest, 23.XI.2001 |
| CR | Computer und Recht (Zeitschrift) |
| ders. | derselbe |
| d. h. | das heißt |
| Dr. | Doktor |
| DVO | Verordnung der Durchführung |
| EG/EU | Europäische Gemeinschaft/Union |
| Einl. | Einleitung |
| EMRK | Europäische Menschenrechtskommission |
| etc. | et cetera |
| EuGH | Europäischer Gerichtshof |
| f./ff. | folgende/fortfolgende |

| | |
|-------------------|--|
| FAG | Gesetz über Fernmeldeanlagen, das am 31. Dezember 2001 außer Kraft getreten ist. |
| Fn. | Fußnote |
| G 10 | Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Art. 10 GG) |
| GA | Goltdammer's Archiv für Strafrecht (Zeitschrift) |
| GG | Grundgesetz |
| ggf. | gegebenenfalls |
| GRCh | Charta der Grundrechte der Europäischen Union |
| h. M. | herrschende/r Meinung |
| Hrsg. | Herausgeber |
| Hs. | Halbsatz |
| i. d. R. | in der Regel |
| i. e. S. | im engeren Sinne |
| insb. | insbesondere |
| i. R. d./i. R. v. | im Rahmen des/der/von |
| i. S. d. | im Sinne des/der |
| ISP | (eng.) Internet Service Provider (= Internetdienstanbieter) |
| IT | Informationstechnik |
| IuK-Technologie | Informations- und Kommunikationstechnologie |
| i. V. m. | in Verbindung mit |
| JA | Juristische Arbeitsblätter (Zeitschrift) |
| JR | Juristische Rundschau (Zeitschrift) |
| JuMoG | 1. Justizmodernisierungsgesetz vom 24. August 2004 (BGBl. I S. 2198) |
| K-DSG | Südkoreanisches Gesetz zum Schutz personenbezogener Daten, das am 4. Februar 2020 parlamentarisch beschlossen und am 5. August 2020 in Kraft getreten ist (Gesetz Nr. 16930) |
| K-KGSG | Südkoreanisches Gesetz zum Schutz des Kommunikationsgeheimnisses, das am 24. März 2020 parlamentarisch beschlossen und in Kraft getreten ist (Gesetz Nr. 17090) |
| <i>K-MRK</i> | Südkoreanische Nationale Menschenrechtskommission |
| <i>K-OGH</i> | Südkoreanischer Oberster Gerichtshof |
| <i>K-OGHE</i> | Entscheidungen des <i>K-OGH</i> |
| krit. | kritisch |
| K-StandODSG | Südkoreanisches Gesetz zur Verwendung und zum Schutz der Standortdaten, das am 8. Dezember 2020 parlamentarisch beschlossen und in Kraft getreten ist (Gesetz Nr. 17633) |
| K-StPO | Südkoreanische Strafprozessordnung, die am 4. Februar 2020 parlamentarisch beschlossen und am 1. Januar 2021 in Kraft getreten ist (Gesetz Nr. 16924) |
| K-TKGG | Südkoreanisches Telekommunikationsgeschäftsgesetz, das am 10. Dezember 2019 parlamentarisch beschlossen und am 11. Juni 2020 in Kraft getreten ist (Gesetz Nr. 16824) |
| K-Verf | Südkoreanische Verfassung, die am 29. Oktober 1987 parlamentarisch beschlossen und am 25. Februar 1988 durch Volksentscheid festgelegt wurde |
| <i>K-VerfG</i> | Südkoreanisches Verfassungsgericht |
| <i>K-VerfGE</i> | Entscheidungen des <i>K-VerfG</i> (Zitiert: <i>K-VerfGE</i> Band-Nummer, erste S., betroffene S.; z. B. <i>K-VerfGE</i> 30–2, 481, 483) |

| | |
|--------------|--|
| LfV | Landesamt für Verfassungsschutz |
| LG | Landgericht |
| lit. | Buchstabe |
| LOStA | Leitender Oberstaatsanwalt |
| MAD | Militärischer Abschirmdienst |
| MMR | Multimedia und Recht (Zeitschrift) |
| m. w. N. | mit weiteren Nachweisen |
| n. F. | neue Fassung |
| NJW | Neue juristische Wochenschrift (Zeitschrift) |
| Nr./Nrn. | Nummer/Nummern |
| NSZ | Neue Zeitschrift für Strafrecht (Zeitschrift) |
| NWVerfSchG | Gesetz über den Verfassungsschutz in Nordrhein-Westfalen |
| o. g. | oben genannt/-e/-er/-es |
| OLG | Oberlandesgericht |
| OrgKG | Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität vom 15. Juli 1992 (BGBl. I S. 1302) |
| OrgKVerbG | Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 4. Mai 1998 (BGBl. I S. 845) |
| Prof. | Professor |
| RFID-Technik | Radio-Frequenz-Identifikations-Technik |
| RL | Richtlinie |
| Rn. | Randnummer |
| Rspr. | Rechtsprechung/-en |
| S. | Satz oder Seite |
| sog. | sogenannte/sogenannter/sogenanntes |
| StA | Staatsanwaltschaft |
| StGB | Strafgesetzbuch |
| StPO | Strafprozessordnung |
| StraFo | Strafverteidiger Forum (Zeitschrift) |
| StV | Strafverteidiger (Zeitschrift) |
| StVÄG 1999 | Gesetz zur Änderung und Ergänzung des Strafverfahrensrechts – Strafverfahrensänderungsgesetz 1999 vom 2. August 2000 (BGBl. I S. 1253) |
| TK | Telekommunikation/-en |
| TKG | Telekommunikationsgesetz |
| TKÜ | Telekommunikationsüberwachung |
| TKÜG | Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der RL 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198) |
| Tz. | Textziffer |
| u. a. | unter anderem |
| VDS | Vorratsdatenspeicherung |
| VE | Verdeckter Ermittler |
| VerfG | Verfassungsgericht |
| vgl. | vergleiche |
| VO | Verordnung |
| WiJ | Journal der Wirtschaftsstrafrechtlichen Vereinigung (Zeitschrift) |
| z. B. | zum Beispiel |

| | |
|-------|---|
| ZD | Zeitschrift für Datenschutz (Zeitschrift) |
| ZIS | Zeitschrift für internationale Strafrechtsdogmatik (Zeitschrift) |
| ZStW | Zeitschrift für die gesamte Strafrechtswissenschaft (Zeitschrift) |
| zust. | zustimmend |

Kapitel 1

Vorbemerkung

A. Ausgangspunkte

I. Aktuelle Lage

Heute ist die Nutzung von IuK-Technologie und darauf basierenden informationstechnischen Systemen wie etwa privaten PCs oder Smartphones und betrieblichen Servern, die durch Internet miteinander verbunden sind, für die Lebensführung der meisten Bürgerinnen und Bürger von zentraler Bedeutung und notwendig. Damit ist in nahezu allen Lebensbereichen eine Effektivität und eine Erleichterung der Geschäftsabwicklung erheblich erhöht. Demzufolge können in einer modernen Informationsgesellschaft ohne die Nutzung der Informationstechnik und der Systeme tatsächlich Einzelpersonen ihre Persönlichkeit nicht frei entfalten, Unternehmen und Organisationen ihre Erwerbstätigkeit nicht frei ausüben und Staaten ihre Aufgaben nicht voll erfüllen. Heute schon sind Einfluss und Bedeutung der IuK-Technologie durchschlagend, weiter wird dies durch die fortwährende Entwicklung und Konvergenz der Technologien immer mehr zunehmen. Unter diesen Gegebenheiten existieren alle Arten von Informationen in Form von elektronischen Daten oder können in diese umgewandelt werden. Mit der Entwicklung digitaler TK-Technologie werden umfangreiche Daten unbegrenzt und kumulativ angesammelt und konzentriert, und auch der Zugriff auf solche Daten ist einfach. Dies stellt den entscheidenden Unterschied gegenüber frühen Kommunikationsbedingungen dar. Sowohl im Bereich der Privatwirtschaft als auch im Bereich öffentlicher Verwaltung werden zahlreiche neuartige Dienste derzeit über das Internet erbracht, dabei werden Spuren der Nutzung, nämlich personenbezogene Daten, nicht nur auf lokalen Geräten, sondern auch auf Servern der Unternehmen und der Staatsorgane weitumfassend gespeichert.

Die informationstechnischen Systeme und das Internet sind daher den Tätern der Gegenstand von Straftaten bzw. die Mittel der Tatbegehung, während sie den Staatsorganen das Ziel des Schutzes bzw. die Mittel wirksamer Aufgabenerfüllung sind. Die Datenspuren in solchen Systemen und im Internet stellen meistens Beweismittel dar, die dem Beweis für die Untersuchung des Sachverhalts dienen, und

daher stehen sie stets im Mittelpunkt des Interesses der Strafverfolgungsbehörden.¹ Heute kann die Ermittlung ohne die Nutzung der IuK-Technologie oder ohne die Untersuchung elektronischer Daten nicht mehr gedacht werden. Für die Verfolgung sowohl von Staatsschutzdelikten oder Wirtschafts- bzw. Steuerkriminalität als auch von klassischen Delikten wie Straftaten gegen das Leben, gegen die körperliche Unversehrtheit oder gegen die sexuelle Selbstbestimmung stellen in der Praxis die zuvorderst zu sichernden Beweismittel die auf den informationstechnischen Systemen und im Internet befindlichen Daten dar. Folglich drängt die Entwicklung der IT die Ermittlungsbehörde, mit neuen Ermittlungsmethoden Schritt zu halten. In Ansehung dieser Ansammlung und Konzentration von Daten können aber die technischen Mittel zur Datenerhebung im Ermittlungsverfahren stets bis hin zu einer Bildung von Persönlichkeitsprofilen bzw. einer Rundumüberwachung führen. Heutzutage bringt die Erfassung personenbezogener Daten durch die Strafverfolgungsbehörden je nach Art des Eingriffs eine spezifische Gefährdung der Persönlichkeit mit sich, damit wird die Intensität des Grundrechtseingriffs viel mehr erhöht als in der Vergangenheit.² Kurzum dient die fortschreitende Entwicklung der IuK-Technologie einerseits der Persönlichkeitsentfaltung der Bürger, andererseits steigert sie aber auch die Gefahr des Eingriffs in die Persönlichkeit erheblich.

Technischer Fortschritt und eine dadurch möglich gemachte staatliche Erhebung und Verwendung umfangreicher Daten wirken auch auf die Struktur des Strafverfahrens. Das Ermittlungsverfahren nimmt im gesamten Strafprozess einen höheren Stellenwert ein als früher, und es wird oft eher wichtiger als die Hauptverhandlung. Das bedeutet, dass die Macht der Strafverfolgungsbehörden in vielen Fällen tatsächlich größeren Einfluss auf das Strafverfahren hat als diejenige des Gerichts. Wenn also das Ermittlungsrecht im Vorverfahren nicht angemessener kontrolliert wird als derzeit, kann eine große Lücke im Grundrechtsschutz entstehen. Darüber hinaus kann diese nicht-kontrollierte Ermittlungsmacht eine Atrophie einer unbefangenen Wahrnehmung der Grundrechte, insb. eine Einschränkung der freien Meinungsäußerung, die liberaler Demokratie zugrunde liegt, nach sich ziehen. Dies rüttelt an den Grundfesten des GG, dem liberalen Rechtsstaat. So muss u. a. „verdeckte bzw. umfangreiche Datenerhebung“ unter dem Rechtsstaatsprinzip angemessen kontrolliert werden. Während der Katalog der strafprozessualen Zwangsmittel in den letzten Jahrzehnten laufend an den rapiden Fortschritt der Ermittlungs- und Überwachungstechniken angepasst und dadurch permanent ausgedehnt worden ist, treten die rechtsstaatlichen Kontrollmechanismen auf der Stelle.³ Mit Blick auf

¹ Vgl. Kudlich, StV 2102, 560, 561: „(es gibt) ... ‚Datenspuren‘ in einem Umfang, wie er früher nie denkbar war, so dass sich die Frage stellt, inwiefern diese für die Strafverfolgungsbehörden nutzbar gemacht werden können.“

² Vgl. Singelstein, NStZ 2012, 593, 594: „Bei neuen technischen Möglichkeiten ... führen die weitergehenden Möglichkeiten der Ausforschung dazu, dass strafprozessuale Eingriffe deutlich mehr und deutlich sensiblere Erkenntnisse erbringen und somit zu tieferen Grundrechtseingriffen führen als früher.“

³ Roxin/Schünemann, § 29 Rn. 25.

den heutigen Stand der Technik führt eine staatliche Erhebung personenbezogener Daten ohne angemessene Kontrolle dazu, den Bürgern Angst vor der Überwachung und der Strafe durch den Staat zu machen und sie an *big brother* – des Romans „1984“ (Autor: *George Orwell*) – zu gemahnen.

II. Historische Übersicht

1. Entstehung und Entwicklung betreffender Vorschriften in Deutschland

Bis 1990 gab es auf dem IuK-Gebiet nur die §§ 99, 100 StPO zur Überwachung von Postsendungen und Telegrammen, die seit Inkrafttreten der Reichsstrafprozessordnung vom 1. Oktober 1879⁴ existieren, und §§ 100a, b StPO a.F. zur Überwachung und Aufzeichnung des Fernmeldeverkehrs, die am 1. November 1968 in Kraft traten, wobei nach der Entscheidung des *BGH* sonstige verdeckte Ermittlungsmaßnahmen zum Zwecke der Strafverfolgung in der StPO grundsätzlich unzulässig waren.⁵ Um den zunehmenden Staatsschutz- oder Wirtschafts- und Steuerdelikten zu begegnen, wurden viele Vorschriften im 8. Abschnitt des Ersten Buches der StPO in den letzten 30 Jahren geschaffen und geändert. Derzeit bestehen in der StPO neben allgemeinen Vorschriften der Durchsuchung und Beschlagnahme von §§ 94 ff., 102 ff. StPO verschiedene Vorschriften zur heimlichen Erhebung personenbezogener Daten. Viele heimliche Überwachungsmaßnahmen, die durch diese Umgestaltungen ermöglicht wurden, geben jedoch den Ermittlungsbehörden gewaltige Befugnisse, in das Persönlichkeitsrecht aller Bürger erheblich einzugreifen. Gerade dies ist heiß umstritten. Zu überblicken ist die Geschichte der Schaffung und Reformen zu heimlichen Ermittlungsmaßnahmen in der StPO wie folgt:⁶

⁴ StPO vom 1. Februar 1877 (RGBl. S. 253).

⁵ Vgl. *BGHSt* 34, 39 (= der 3. Strafsenat des *BGH*, Urteil vom 9. April 1986 – 3 StR 551/85 –): ein Verwertungsverbot der heimlichen Aufnahme nichtöffentlicher Gespräche des Beschuldigten zwecks Stimmanalyse. Das Urteil betrifft die Zulässigkeit von Beweismitteln bei der Verurteilung wegen der Ermordung eines Mitglieds der „Roten Armee Fraktion“ (RAF: 1970–1998), einer linksextremistischen terroristischen Vereinigung.

⁶ Bemühungen, gegen die von der Technik gewandelte Realität vorzugehen, laufen sowohl auf nationaler Ebene als auch auf internationaler Ebene zugleich. Denn zur Verfolgung der Tat im Cyberspace ist wegen transnationaler Aktionsmöglichkeiten der IuK-Technologie (Internationalität) und territorialer Beschränkung der Ermittlungshandlung als Hoheitsakt eine internationale Kooperation notwendig. Auch auf europäischer Ebene wurde in den letzten mehr als zwanzig Jahren eine Diskussion über die Ausgestaltung der Rechtsgrundlage zum Schutz der durch die IuK-Technologie erstellten, verarbeiteten, gespeicherten und übermittelten Daten und zum Zugriff darauf geführt und sie wird noch immer geführt: RL 95/46/EG, 97/66/EG, 2002/58/EG, 2005/222/JI, 2006/46/EG, 2013/40/EU, 2016/680/EU und VO 2016/679/EU der Europäischen Union und CKÜ vom Europarat sowie auch Entscheidungen vom *EuGH*. Durch diese Serie von Bestrebungen wurde materielles Strafrecht in der EU zum großen Teil vereinbart, hingegen prozessuales Recht nicht (*Sieber*, 69. DJT 2012, C 12). Denn eine straf-